Titre: Title:	Problèmes combinatoires reliés aux problèmes d'affectation de fréquences et de codage
Auteur: Author:	Maurice Morel
Date:	2006
Type:	Mémoire ou thèse / Dissertation or Thesis
Référence: Citation:	Morel, M. (2006). Problèmes combinatoires reliés aux problèmes d'affectation de fréquences et de codage [Ph.D. thesis, École Polytechnique de Montréal]. PolyPublie. https://publications.polymtl.ca/7795/

UNIVERSITÉ DE MONTRÉAL

PROBLÈMES COMBINATOIRES RELIÉS AUX PROBLÈMES D'AFFECTATION DE FRÉQUENCES ET DE CODAGE

MAURICE MOREL
DÉPARTEMENT DE MATHÉMATIQUES ET DE GÉNIE INDUSTRIEL
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

THÈSE PRÉSENTÉE EN VUE DE L'OBTENTION
DU DIPLÔME DE PHILOSOPHIÆ DOCTOR (Ph.D.)
(MATHÉMATIQUES DE L'INGÉNIEUR)
DÉCEMBRE 2006

Your file Votre référence
ISBN: 978-0-494-24543-9
Our file Notre référence
ISBN: 978-0-494-24543-9

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Cette thèse intitulée :

PROBLÈMES COMBINATOIRES RELIÉS AUX PROBLÈMES D'AFFECTATION DE FRÉQUENCES ET DE CODAGE

présentée par : MOREL Maurice

en vue de l'obtention du diplôme de : Philosophiæ Doctor

a été dûment acceptée par le jury d'examen constitué de :

M. HERTZ Alain, Doct. ès Sc., président

Mme JAUMARD Brigitte, T. Doct., T. Hab., membre et directrice de recherche

Mme MARCOTTE Odile, Ph.D., membre et codirectrice de recherche

M. SOUMIS François, Ph.D., membre

M. WALSH Timothy, Ph.D., examinateur externe

REMERCIEMENTS

Je tiens tout d'abord à remercier Mme Jaumard et Mme Marcotte pour m'avoir dirigé tout au long de la rédaction de cette thèse.

Je remercie chaque membre de ma famille pour leur présence durant cette période et plus particulièrement ma copine Julie pour m'avoir épaulé lorsqu'il en était temps.

Je remercie mes amis et confrères pour leur présence et pour les pauses passées ensemble.

Finalement, je tiens à remercier tout spécialement Chritophe Meyer pour m'avoir offert son temps et ses conseils dans le domaine de la programmation linéaire.

RÉSUMÉ

Dans cette thèse nous avons étudié deux problèmes combinatoires reliés au problème d'affectation de fréquences. Nous avons tout d'abord investigué le problème de la T-coloration. La notion de T-coloration d'un graphe est utilisée pour modéliser une simplification du problème d'affectation de fréquences. La T-étendue optimale d'un graphe G représente la largeur de bande nécessaire pour avoir une affectation valide pour le réseau représenté par G. Dans la première partie de cette thèse nous avons déterminé des classes de graphes pour lesquelles nous pouvions facilement calculer la T-étendue.

Le reste de la thèse a été consacrée au problème de la règle de Golomb et à différentes généralisations de ce problème. Nous avons premièrement exposé de façon rigoureuse le fonctionnement des méthodes algébriques à l'aide de géométries finies puis, à partir de cette théorie, nous avons implémenté une heuristique pour construire des règles de Golomb. En généralisant la théorie aux géométries finies de dimensions supérieures, nous avons obtenu une heuristique pour la construction des ensembles doublements orthogonaux, ensembles qui ont leur utilité en théorie du codage. Nous avons obtenu dans la plupart des cas, des améliorations significatives sur la longueur des ensembles doublement orthogonaux.

La dernière partie de la thèse a été reservée au problème des ensembles de différences triangulaires (DTS), une autre généralisation du problème de la règle de Golomb qui est utilisée en théorie du codage. Pour améliorer les bornes inférieures sur la longueur des DTS, nous avons construit un modèle utilisant la génération de colonnes. Une implémentation de ce modèle nous a fourni, pour les petites valeurs, les meilleures bornes inférieures obtenues par la programmation linéaire.

ABSTRACT

In this thesis we have studied two combinatorial problems related to the frequency assignment problem. We first investigated the T-coloring problem. Graph T-coloring is used to model a simplification of the frequency assignment problem. The optimal T-span of a graph G is used to represent the necessary band-width to have a valid assignment for the network represented by G. In the first part of this thesis we determined some classes of graphs for which we can easily compute the T-span.

The rest of this thesis is concerned with the Golomb ruler problem and generalizations of it. We exposed rigorously an algebraic method, based on finite geometries, that we use to generate and study Golomb rulers. By generalizing the theory to finite geometries of higher dimensions, we obtained a heuristic for the generation of doubly orthogonal sets, which are used in coding theory. In most of the cases, we obtained significant improvements on their lengths.

The last part of this thesis is concerned with the DTS problem, another generalization of the Golomb ruler problem, used in coding theory. To improve the lower bounds of the DTS lentghs we built a model using column generation. We obtain, for small values, the best lower bounds from linear programming.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

TABLE DES FIGURES

LISTE DES ALGORITHMES

INTRODUCTION

Depuis quelques décennies, le domaine des communications a connu un essor extraordinaire grâce à la découverte de nouvelles technologies. Cet essor a fourni aux chercheurs une grande quantité de problèmes théoriques inhérents à la mise en place de ces nouvelles technologies. La résolution de ces problèmes représente parfois un niveau de rentabilité suffisant pour déterminer si les technologies sous-jacentes peuvent être mises en place ou non. L'économie mondiale actuelle ainsi que notre qualité de vie dépend en grande partie de l'efficacité de l'échange d'information. La recherche de meilleures méthodes de résolution pour les problèmes reliés aux technologies déjà mises en place est donc aisément validée.

Le problème d'affectation de fréquences (PAF) figure parmi les problèmes importants dans le domaine des communications. Ce problème consiste à affecter à un ensemble d'émetteurs-récepteurs, situés dans un réseau, des fréquences appartenant à un certain spectre de manière à éviter les interférences entre les différentes émissions d'ondes. L'importance de ce problème vient du fait que les besoins de communication sont toujours croissants, ce qui correspond à une complexification du réseau d'émetteurs-récepteurs, alors que le spectre des fréquences radio est une ressource fixe.

Dans les applications de la vie courante, les contraintes de PAF peuvent varier selon la qualité d'émission nécessaire pour le bon fonctionnement de l'application. De même, la difficulté de résolution du problème varie selon les exigences imposées. Différentes variations du problème PAF peuvent également être envisagées selon que les applications dépendent d'un réseau permanent ou variable. Pour résoudre les différentes variantes de PAF, des modèles doivent être construits. Une des approches pour résoudre PAF dans le cas général est la méthode des T-colorations introduite

par Hale (1980). La notion de T-coloration est une généralisation de la notion usuelle de coloration de graphe, où T fait simplement référence à un ensemble de valeurs interdites correspondant à des intervalles du spectre des fréquences qui doivent être évités.

La méthode de résolution de PAF à l'aide des T-colorations n'est pas complète, dans le sens où toutes les contraintes relatives au réseau ne peuvent pas être considérées par le problème de la T-coloration. De façon générale, les contraintes associées au problème PAF sont des contraintes d'interférence. L'interférence est le phénomène qui survient lorsque plusieurs signaux se mêlent pour former un nouveau signal indésirable. Un type particulier d'interférence qui survient dans les applications pratiques et qui ne peut pas être considéré avec les T-coloration est l'intermodulation. L'intermodulation est le phénomène d'interférence qui survient lorsque plusieurs signaux se mêlent pour former un nouveau signal de fréquence près d'une fréquence existante, ceci empêche alors le signal d'être filtré, et par conséquent, les signaux originaux d'être retrouvés. On distingue différents types d'intermodulation selon le nombres de signaux en cause. En théorie tous les produits d'intermodulation possibles doivent être considérés pour résoudre le problème de l'intermodulation, mais en pratique la résolution du problème n'est faite que pour un nombre borné de signaux pouvant se combiner.

En considérant la formulation du problème de l'intermodulation donnée par Babcock (1953), le problème peut être décomposé et traduit en terme de problèmes combinatoires s'apparentant aux règles de Golomb. En effet, lorsque le signal de chaque émetteur est susceptible de produire de l'intermodulation, le problème de l'intermodulation d'ordre 3, c'est-à-dire avec au plus trois signaux se combinant, se résume à trouver une régle de Golomb avec un nombre d'entiers correspondant au nombre d'émetteurs. De même, le problème de l'intermodulation pour les ordres supérieurs peut également être traité avec des notions généralisant les règles de Golomb (Atkinson et al., 1986).

Dans cette thèse nous nous sommes intéressés de façon théorique à deux sous-problèmes du problème PAF. Le premier sous-problème est l'affectation des fréquences en ne tenant compte que des contraintes sur les différences entre les fréquences qui doivent être affectées. Comme nous l'avons déjà dit, ce problème est équivalent au problème de T-coloration sur les graphes. Le second sous-problème est le problème d'intermodulation ou, sous la forme que nous l'avons abordé, le problème de la règle de Golomb. Nous avons également considéré certaines généralisations du problème de la régle de Golomb, c'est-à-dire les ensembles doublement orthogonaux et les ensembles de différences triangulaires.

Le premier chapitre de cette thèse est uniquement consacré au problème de la T-coloration de graphes. La première section de ce chapitre consiste en une brève mise en situation. Dans la seconde section nous présentons les notions générales concernant le problème PAF : énoncé du problème, explication des différents types d'interférence, présentation des contraintes associées à chaque type d'interférence ainsi qu'un aperçu des modèles utilisés pour résoudre les problèmes. Dans la troisème section nous présentons d'abord les définitions et les résultats de bases concernant les graphes et les T-colorations, puis la section se termine sur la présentations des dernières avancées sur le sujet des T-colorations. La quatrième section qui est consacrée aux homomorphismes de graphes est utile pour expliquer et justifier les résultats de la section suivante. Dans la cinquième section de ce chapitre nous présentons les résultats que nous avons obtenus concernant les classes de graphes pour lesquels il est possible de résoudre le problème de la T-coloration de manière efficace, c'est-à-dire avec des algorithmes polynomiaux. Puis nous terminons cette section par un algorithme polynomial que nous avons obtenu pour déterminer une borne sur les T-colorations des graphes 3-colorables à partir de la seule donnée d'un ensemble T de valeurs interdites.

Le second chapitre de cette thèse porte sur un problème combinatoire ayant de nombreuses applications, le problème de la règle de Golomb. Une application de ce problème est, comme nous l'avons déjà dit, le traitement de l'intermodulation d'ordre

3 dans le problème PAF. La première section de ce chapitre constitue une mise en situation du problème. Premièrement, le problème est défini, puis nous présentons les applications des règles de Golomb, les bornes du problème sont ensuite discutées, et finalement, cette section se termine par la présentation des différentes approches pour résoudre ce problème. La seconde section donne un bref aperçu des méthodes de résolution dites exactes. La troisième section de ce chapitre présente de façon formelle les méthodes algébriques pour construire les règles de Golomb. La première partie contient les résultats sur les corps finis qui nous seront utiles pour justifier le recours aux méthodes algébriques pour solutionner le problème de la règle de Golomb. Nous présentons ensuite les différentes constructions pour les géométries finies ainsi que les résultats relatifs à ces géométries. Finalement, nous présentons les algorithmes de constructions des règles de Golomb basés sur les méthodes algébriques. Cette partie de la thèse à pour avantage de présenter au lecteur de façon explicite les idées sous-jacentes aux méthodes algébriques. Il existe en effet dans la littérature de nombreuses références sur les méthodes algébriques mais les explications sont, dans la plupart des cas, insuffisantes. Les travaux de cette partie visent donc également à remplir cette lacune. La quatrième section de ce chapitre porte sur les ensembles doublement orthogonaux, une notion généralisant la notion de règle de Golomb qui correspond au problème de l'intermodulation pour les ordres supérieurs . Dans cette section, nous présentons tout d'abord quelques résultats utiles sur les corps finis. Nous présentons ensuite les relations liant les géométries finies à la structure des ensembles doublement orthogonaux. La partie suivante est consacrée à l'algorithme de construction des droites pour les géométries finies. Nous présentons ensuite un algorithme pour réduire les ensembles doublement orthogonaux obtenus par les géométries finies. Puis, la dernière partie de cette section est réservée à la présentation des résultats obtenus par nos algorithmes. Ces algorithmes fournissent dans la plupart des cas les meilleurs ensembles doublement orthogonaux connus à ce jour.

Le troisième chapitre de cette thèse est consacré au problème des ensembles de différences triangulaires (DTS), une généralisation des règles de Golomb. La première

section de ce chapitre est utilisée pour énoncer les généralités sur les DTS. Nous présentons tout d'abord la définition du problème, puis les propriétés générales. Nous discutons ensuite brièvement des applications des DTS. Puis nous donnons les bornes connues pour le problème des DTS. La section se termine sur un bref aperçu des approches existantes pour résoudre le problème du DTS. La seconde section est dédiée aux méthodes algébriques. Nous présentons en premier lieu les différentes notions d'algèbre inhérentes au sujet. Puis, dans le reste de cette section nous présentons les différentes techniques algébriques pour lesquelles les meilleurs DTS sont obtenus. La troisième section concerne les méthodes de résolutions relatives à la programmation linéaire. Nous présentons d'abord le premier modèle de programmation linéaire proposé par Lorentzen et Nilsen (1991) et ensuite une formulation révisée de leur modèle. Puis, cette section ce termine par la présentation d'une formulation améliorée du modèle de Lorentzen et Nilsen proposée par Shearer (1999). La quatrième section de ce chapitre concerne une formulation que nous avons proposée, basée sur le principe de la génération de colonnes. Nous présentons premièrement notre formulation en détail, puis nous démontrons la validité de notre modèle. Nous présentons ensuite les résultats obtenus avec notre formulation concernant la borne inférieure sur les DTS. Les différentes améliorations apportées à notre modèle fournissent dans quelques cas les meilleures bornes inférieures connues à ce jour et, de façon générale, les meilleures bornes inférieures obtenues par programmation linéaire.

CHAPITRE 1

HOMOMORPHISMES ET T-COLORATIONS

1.1 Introduction

Dans le domaine de la théorie des graphes, le problème de coloration des graphes a été étudié par plusieurs chercheurs. De nombreux travaux sur le sujet sont disponibles, et le lecteur intéressé peut se référer au livre de Jensen et Toft (1995). Ce problème a de nombreuses applications dans la vie courante. Pour ne donner que quelques exemples, citons les problèmes d'affectation de tâches, de maintenance de flottes, de réglage de feux de circulation, de collecte d'ordures, de confection d'horaires, etc. (Roberts, 1991a). Il est bien connu que le problème de coloration des graphes appartient à la classe des problèmes NP-complets (Garey et Johnson, 1979). Par conséquent, il n'existe pas à ce jour d'algorithme pour résoudre ce problème en temps polynomial. Ainsi, le problème de coloration des graphes demeure toujours un sujet d'actualité. Une généralisation de la notion de coloration des graphes est le problème de la T-coloration des graphes. La notion de T-coloration a été introduite par Hale (1980) pour modéliser le problème d'affectation de fréquences.

1.2 Problème d'affectation de fréquences

Étant donné un ensemble d'émetteurs radio $V = \{1, 2, ..., n\}$, un spectre radio R et un ensemble de contraintes, le problème d'affectation de fréquences, en abrégé PAF, consiste à affecter à chaque émetteur une fréquence disponible dans le spectre, de manière à respecter chacune des contraintes données. De façon générale, les contraintes

du problème sont définies par les interférences qui surviennent entre les émetteurs. Ces contraintes portent donc sur les différences entre les fréquences qui sont affectées aux émetteurs. Soit V l'ensemble des émetteurs. Une fonction $f : V \rightarrow R$ qui satisfait les contraintes imposées est appelée une *affectation de fréquences.* Le problème d'affectation de fréquences est un problème très difficile, c'est-à-dire NP-complet (Hale, 1980; Garey et Johnson, 1979). Pour cette raison plusieurs simplifications du problème ont été considérées dans les différentes études sur le sujet. Dans cette section, nous utilisons une terminologie due à Hale (1980), qui a été le premier à réaliser l'unification des différents résultats se rapportant au problème PAF. De même, nous ne considérons le problème que dans le cas où chaque émetteur est omnidirectionnel, les émetteurs sont tous de même puissance et ils disposent tous de la même largeur de bande. Cette dernière simplification nous permet donc de considérer l'ensemble des fréquences disponibles comme étant un sous-ensemble fini de $\mathbb{Z}^+$.

1.2.1 Types des contraintes

Soit V un ensemble d'émetteurs et f une affectation de fréquences, on classe les contraintes sur $\{u, v\}$, une paire d'émetteurs, selon la plus petite différence permise entre $f(u)$ et $f(v)$ de manière à ce qu'il n'y ait pas d'interférence entre u et v. En particulier, on dit qu'on a une contrainte co-canal entre deux émetteurs u et v lorsqu'on ne peut pas affecter la même fréquence à u et v sans qu'il y ait d'interférence. Lorsque les deux émetteurs u et v doivent avoir des fréquences qui diffèrent de plus de 1 pour éviter l'interférence, on parle de contraintes d'adjacence entre u et v. De façon générale, lorsque les deux émetteurs doivent avoir des fréquences qui diffèrent de plus de k, on a une contrainte d'adjacence de niveau k.

Dans une version simplifiée du problème PAF, les contraintes d'interférence sont toutes définies par rapport aux distances entre les émetteurs. Ainsi, une contrainte de co-canal s'exprime comme $D(u, v) \leq d \Rightarrow |f(u) - f(v)| \neq 0$. Autrement dit,

si u et v se situent à moins de d kilomètres l'un de l'autre, alors ils doivent avoir des fréquences différentes. Une contrainte d'adjacence de niveau k s'exprime comme $D(u,v) \leq d \Rightarrow |f(u) - f(v)| > k$.

Hale (1980) a donné une terminologie unificatrice pour tous les problèmes d'affectation de fréquences ayant un certain type de contraintes. La formulation du problème PAF qui suit est une généralisation des différents problèmes d'affectation de fréquences définis par rapport aux distances. La contrainte générale de niveau k est : $R(k) = (T(k), d(k))$, où $k = 0, 1, 2, ..., m$, $T(k) \subseteq \mathbb{Z}^+$ est un ensemble fini et $d(k) \in \mathbb{Z}^+$ pour tout k. Les $T(k)$ et les $d(k)$ doivent satisfaire

$$\{0\} = T(0) \subseteq T(1) \subseteq ... \subseteq T(m) \text{ et}$$

$$d(0) > d(1) > ... > d(m) > 0.$$

Alors, si $|f(u) - f(v)| \notin T(k), \forall u, v \in V$, on dit que f est une *affectation de fréquences* pour V et $T(k)$.

Pour les cas où les contraintes ne sont pas définies par rapport aux distances, Hale construit un ensemble de contraintes encore plus général que le précédent, contenu dans une matrice appelée matrice de séparation des canaux.

Définition 1.1. *Soit* $V = \{1, 2, ..., n\}$ *l'ensemble des émetteurs et soit*

$$\mathcal{P}^*(\mathbb{Z}^+) = \{S \subseteq \mathbb{Z}^+ \mid S = \emptyset \text{ ou } S \text{ est un ensemble fini contenant } 0\}.$$

Si $t : V \times V \rightarrow \mathcal{P}^*(\mathbb{Z}^+)$ *satisfait* $t(i,i) = \emptyset$ *et* $t(i,j) = t(j,i)$ *pour tout* $i, j \in V, i \neq j$, *alors* t *est appelée la* matrice de séparation des canaux *pour* V. *Si* $f : V \rightarrow \mathbb{Z}^+$ *satisfait* $|f(i) - f(j)| \notin t(i,j)$, $\forall i, j \in V$ *alors* f *est appelée une* affectation réalisable *pour* V *et* t.

1.2.2 Applications des T-colorations

Une T-coloration d'un graphe G est une coloration des sommets de G avec des entiers telle que la différence entre les couleurs de n'importe quelle paire de sommets

n'appartiennent pas à T, un ensemble d'entiers. La définition des contraintes du problème d'affectation de fréquences montre de façon évidente la relation entre le problème de T-coloration et le problème PAF. Ce chapitre, suite à la présentation du problème PAF, est consacré à l'étude des T-colorations. Nous y présentons d'abord les définitions et résultats relatifs à cette notion, puis nous déterminons certaines classes de graphes, c'est-à-dire de réseaux de télécommunication, pour lesquelles le problème de T-coloration (et donc le problème PAF) est de résolution facile.

L'obtention de classes de graphes facilement T-colorables permet de calculer des bornes sur le nombre de fréquences nécessaires et l'étendue des fréquences à utiliser. Les bornes fournies peuvent aider à déterminer si le problème possède une solution réalisable pour un spectre radio donné. De même, advenant le cas où aucune solution réalisable n'existe, les algorithmes de T-coloration peuvent grandement faciliter la tâche de déterminer quelles sont les contraintes les plus contraignantes et le cas échéant, réduire ces contraintes tant qu'il n'y a pas espoir de trouver une solution réalisable.

1.2.3 Mécanismes d'interférence et intermodulation

Le problème d'affectation de fréquences tel que présenté précédement se traduit en termes de T-coloration sur les graphes. Toutefois, comme on peut l'imaginer, la résolution d'un tel problème est d'une certaine manière une résolution partielle du problème pratique réel. En effet, dans la formulation générale de PAF, on retrouve certains types de contraintes qui ne sont pas énoncées dans le modèle de la section précédente. Un exemple de contraintes ignorées dans ce modèle est donné par les contraintes d'intermodulation. Pour bien expliquer le mécanisme d'intermodulation, nous présentons d'abord la terminologie se rapportant au modèle que nous utilisons.

Le problème est tout d'abord fourni avec un réseau de télécommunication. Ce réseau est constitué d'un ensemble de sites. Un site est constitué lui-même d'un

ensemble de cellules, et chaque cellule possède un ensemble d'émetteurs. De façon générale, chaque cellule comprend entre 1 et 4 émetteurs. La Figure 1.1 illustre un réseau de 3 sites S_1, S_2 et S_3, où S_1 et S_3 sont des sites à trois cellules et S_2 est un site à deux cellules. Dans cette illustration, chaque cellule possède deux émetteurs.

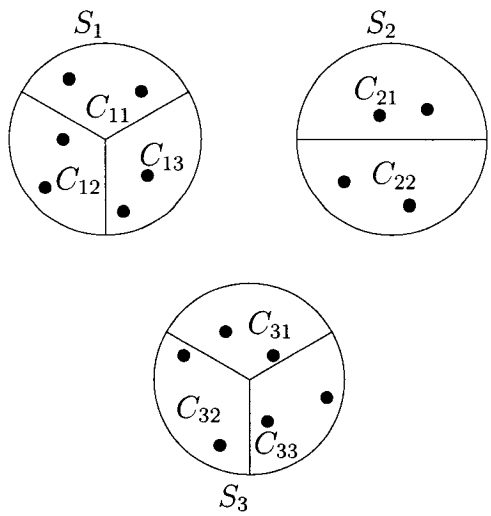

FIGURE 1.1 – *Exemple d'un réseau de télécommunication.*

Lorsqu'on détermine les contraintes d'interférence, on distingue généralement les différents types de mécanismes d'interférence. Un de ces mécanismes est l'interférence co-site. Ce mécanisme qui est illustré à la Figure 1.2 survient, comme son nom l'indique, lorsque deux émetteurs i et j sont situés dans un même site. La Figure 1.2 représente quatre émetteurs, u, v, x et y, avec v et x qui appartiennent au même site. Supposons que u émet un signal pour x et que v émet pour y, puisque les signaux émis par les émetteurs sont omnidirectionnels x reçoit en même temps les signaux de u et de v. Lorsque les signaux sont de longueur d'onde relativement près l'une de l'autre il est possible que le signal reçu par x, qui est alors une combinaison des signaux émis par u et v, soit incompréhensible. Dans ce cas, on dit que les fréquences affectées à x et v doivent être distinctes par au moins d unités. Puisque x et v sont situés dans un même site, la contrainte est alors appelée contrainte d'interférence co-site. Lorsque l'interférence survient entre deux émetteurs issus de sites différents, on dit alors qu'on a une interférence site-disjoint. La raison de la distinction entre

ces deux types d'interférences, qui dans les faits représentent le même phénomène, est que la différence exigée entre deux fréqunces, c'est-à-dire la valeur de d, n'est habituellement pas du même ordre de grandeur pour une contrainte co-site et une contrainte site-disjoint.

Les contraintes associées à ce genre d'interférences prennent habituellement la forme $|f(i)-f(j)| \geq d$, pour d un entier naturel, c'est-à-dire que la fréquence affectée à l'émetteur i doit être distincte par au moins d unités de la fréquence affectée à l'émetteur j . Autrement dit, sous la forme matricielle de la définition 1.1, on aura $t(i,j) = \{0, 1, ..., d-1\}$.

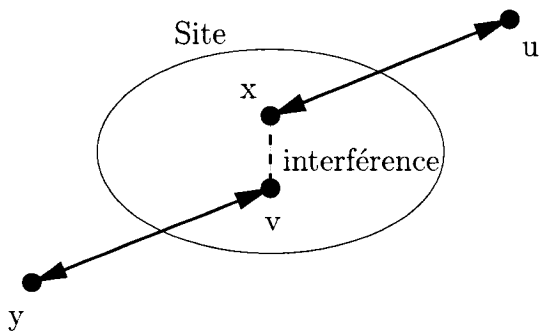

FIGURE 1.2 – *Interférence co-site.*

Un autre mécanisme d'interférence est l'intermodulation. Ce phénomène survient lorsque plusieurs signaux se mêlent de façon à former un nouveau signal indésirable. On peut, en général, filtrer le nouveau signal ainsi formé. Toutefois, s'il s'avère qu'un des signaux produisant l'intermodulation soit assez près du nouveau signal indésirable, la filtration peut devenir impossible sans qu'il n'y ait perte d'information. La Figure 1.3 illustre le phénomène d'intermodulation, où une combinaison des signaux émis par les émetteurs v et w se confond avec le signal émis par u, qui, par conséquent, est impossible à filtrer par le récepteur x. Dans ce cas, on a $|\alpha f(v) + \beta f(w)| = f(u)$, où α et β sont des entiers non nuls et f est l'affectation de fréquence utilisée.

De façon générale, on exprime une contrainte d'intermodulation sous la forme

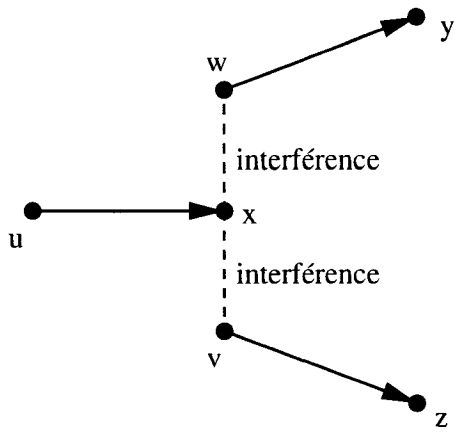

FIGURE 1.3 – *Interférence par intermodulation.*

suivante :

$$\sum_{i=1}^{n} \alpha_i f(x_i) \neq f(y), \text{ où } \alpha_i \in \mathbb{Z}^*, \forall i.$$

On dit alors qu'on a une contrainte de n signaux et d'*ordre* $\sum_{i=1}^{n} |\alpha_i|$. Par exemple, $2f(x_1) + f(x_2) - 2f(x_3) \neq f(y)$ est une contrainte d'intermodulation d'ordre 5 sur 3 signaux. Il est facile de voir que les contraintes d'intermodulation ainsi définies sont très nombreuses, et il devient rapidement fastidieux de toutes les satifaire pour un problème relativement grand. En ce qui nous concerne, nous nous limiterons donc aux contraintes de troisième ordre seulement. Parmi les contraintes de troisième ordre, on distingue d'abord les contraintes de deux signaux et les contraintes de trois signaux. Soit M^{int} la matrice exprimant les contraintes d'intermodulation définie de la façon suivante :

$$M_{ij}^{int} = \begin{cases} 1 & \text{si les produits d'intermodulation créés dans la cellule } C_i \\ & \text{doivent être évités dans la cellule } C_j, \\ 0 & \text{sinon.} \end{cases}$$

On suppose que $M_{ii}^{int} = 0$, pour tout i. Parmi les contraintes de deux signaux, on distingue les deux formes suivantes :

Formulation 1. *Soient C_i et C_j deux cellules telles que $M_{ij}^{int} = 1$. Alors, quelles que soient les fréquences f et f' affectées à la cellule C_i, les fréquences $2f - f'$ et $2f' - f$ ne doivent pas être affectées à la cellule C_j.*

Formulation 2. *Soient C_{i_1}, C_{i_2} et C_j trois cellules telles que C_{i_1} et C_{i_2} appartiennent au même site et $M_{i_1j}^{int} = M_{i_2j}^{int} = 1$. Alors, quelles que soient la fréquence f affectée à C_{i_1} et la fréquence f' affectée à la cellule C_{i_2}, les fréquences $2f - f'$ et $2f' - f$ ne doivent pas être affectées à la cellule C_j.*

En ce qui concerne les contraintes trois signaux, on distingue les trois formes suivantes :

Formulation 1. *Soient C_i et C_j deux cellules telles que $M_{ij}^{int} = 1$. Alors, quelles que soient les fréquences f, f' et f'' affectées à la cellule C_i, les fréquences $f + f' - f''$, $f + f'' - f'$ et $f' + f'' - f$ ne doivent pas être affectées à la cellule C_j.*

Formulation 2. *Soient C_{i_1}, C_{i_2} et C_j trois cellules telles que C_{i_1} et C_{i_2} appartiennent au même site et $M_{i_1j}^{int} = M_{i_2j}^{int} = 1$. Alors, quelles que soient les fréquences f et f' affectées à la cellule C_{i_1} et la fréquence f'' affectée à la cellule C_{i_2}, les fréquences $f + f' - f''$, $f + f'' - f'$ et $f' + f'' - f$ ne doivent pas être affectées à la cellule C_j.*

Formulation 3. *Soient C_{i_1}, C_{i_2}, C_{i_3} et C_j quatre cellules telles que C_{i_1}, C_{i_2} et C_{i_3} appartiennent au même site et $M_{i_1j}^{int} = M_{i_2j}^{int} = M_{i_3j}^{int} = 1$. Alors, quelles que soient la fréquence f affectée à la cellule C_{i_1}, la fréquence f' affectée à la cellule C_{i_2} et la fréquence f'' affectée à la cellule C_{i_3}, les fréquences $f + f' - f''$, $f + f'' - f'$ et $f' + f'' - f$ ne doivent pas être affectées à la cellule C_j.*

Remarque 1.2. *On remarque que le cas à deux signaux est en fait un cas particulier du cas à trois signaux lorsqu'on permet à deux fréquences d'être les mêmes. Il est donc possible de se restreindre aux contraintes de trois signaux pour caractériser les contraintes d'intermodulation de troisième ordre.*

1.2.4 Applications des règles de Golomb

En télécommunications, les règles de Golomb interviennent lorsqu'on considère les produits d'intermodulation de troisième ordre. On a vu précédemment que les contraintes d'intermodulation de troisième ordre s'expriment de façon générale sous la forme $f_1 + f_2 - f_3 \neq f_4$, c'est-à-dire $f_2 - f_3 \neq f_4 - f_1$. Ainsi, lorsqu'on considère un réseau avec un sous-ensemble d'émetteurs présentant toutes les containtes d'intermodulation possibles, le problème de satisfaire ces contraintes se résume à trouver une règle de Golomb. Autrement dit, le fait de considérer toutes les contraintes d'intermodulation correspond à travailler sur un graphe complet G^{int} (graphe des contraintes d'intermodulation) dont les sommets représentent les émetteurs et les arêtes, les contraintes d'intermodulation. Dans le cas où les contraintes d'intermodulations ne sont pas toutes considérées G^{int} n'est pas un graphe complet et alors la longueur minimale d'une règle de Golomb qui a pour ordre le nombre d'émetteurs du réseau est une borne supérieure sur ces composantes. De façon générale, pour les contraintes d'intermodulation d'ordre supérieur à 3 on peut se référer à un article de Atkinson et al. (1986).

Le problème de la règle de Golomb est le sujet d'étude du chapitre 2. On y présente les différentes approches pour le résoudre et les résultats connus.

1.2.5 Remarques sur le cas réel

Le problème d'affectation de fréquences limité aux différences interdites, qui peut être traduit en termes de T-colorations, est considérablement alourdi lorsque l'on considère les contraintes d'intermodulation telles que décrites ci-dessus. Ainsi, lorsqu'on ajoute les contraintes d'intermodulation au problème PAF, le problème se traduit en un problème de T-coloration avec contraintes supplémentaires. Ces contraintes supplémentaires ne s'expriment pas directement en termes de contraintes

de T-coloration et sont d'autant plus difficiles à manipuler. En pratique, pour résoudre ce genre de problèmes, on essaie de limiter le plus possible les phénomènes d'intermodulation, de manière à maintenir les interférences dans le réseau à un niveau acceptable. De plus, puisqu'en pratique le spectre radio utilisable est limité, il devient souvent impossible de trouver une solution réalisable du problème PAF en considérant toutes les contraintes d'intermodulation et en utilisant le spectre radio fourni.

1.3 Graphes et T-colorations

Dans ce qui suit nous présentons les définitions générales de la théorie des graphes et les notations qui seront utilisées tout au long de ce texte. Par la suite, nous énonçons le problème de T-coloration, qui est notre principal sujet d'étude, ainsi que les définitions qui y sont rattachées. Nous présentons ensuite, brièvement, différentes notions relatives aux T-colorations.

1.3.1 Définitions sur les graphes

Un *graphe simple* G est un couple formé d'un ensemble fini V de *sommets* et d'un ensemble de paires de sommets appelées *arêtes*. Dans ce qui suit, nous utilisons *graphe* plutôt que graphe simple, et il sera parfois permis que V soit infini. Étant donné G, on note $V(G)$ l'ensemble des sommets de G et $E(G)$ l'ensemble des arêtes. L'*ordre* d'un graphe G, noté $|G|$, est la cardinalité de $V(G)$.

Soit x et y deux sommets de G. On dit que x et y sont *adjacents* si $\{x, y\} \in E(G)$. Le *voisinage* de $W \subset V(G)$ dans G, noté $N(W)$, est l'ensemble des sommets de $V(G) \setminus W$ qui sont adjacents à au moins un sommet de W. En particulier, le *degré* d'un sommet v, noté $\deg(v)$, est la cardinalité de $N(\{v\})$. Notons que le voisinage d'un

ensemble de sommets est également un ensemble de sommets ; il est donc possible de considérer le voisinage d'un voisinage. L'ensemble obtenu en considérant $i-1$ fois le voisinage du voisinage obtenu en partant de $W \subset V(G)$ est appelé le i-ième voisinage de W et est noté $N^i(W)$.

Le *cycle* d'ordre n, noté C_n, est le graphe défini par $V(C_n) = \{v_1, v_2, ..., v_n\}$ et $E(C_n) = \{\{v_1, v_2\}, \{v_2, v_3\}, ..., \{v_n, v_1\}\}$. Le *graphe complet* d'ordre n, noté K_n, est le graphe défini par $V(K_n) = \{v_1, v_2, ..., v_n\}$ et $E(K_n) = \{\{u, v\} : u, v \in V(K_n), u \neq v\}$.

On dit qu'un graphe H est un *sous-graphe* de G si $V(H) \subseteq V(G)$ et $E(H) \subseteq E(G) \cap (V(H) \times V(H))$. Soit G un graphe et soit $X \subseteq V(G)$. Le *sous-graphe de G induit par X*, noté $G[X]$, est défini par $V(G[X]) = X$ et $E(G[X]) = E(G) \cap \mathcal{P}_2(X)$, où $\mathcal{P}_2(X)$ est l'ensemble des paires d'éléments de X. On dit que H est un *graphe partiel* de G si $V(H) = V(G)$ et $E(H) \subseteq E(G)$. Une *clique* de G est un sous-graphe de G qui est un graphe complet. Une clique X est dite *maximale* si pour tout $v \in V(G) \setminus V(X)$, $G[V(X) \cup \{v\}]$ n'est pas une clique et on note $\omega(G)$ l'ordre maximal d'une clique de G.

Définition 1.3. *Soit G et H deux graphes. Un* homomorphisme *de G dans H, noté $G \to H$, est une fonction $f : V(G) \to V(H)$ telle que pour tous sommets x et y de G, si $\{x, y\}$ est une arête de G alors $\{f(x), f(y)\}$ est une arête de H. De plus, si f est une bijection et si f^{-1} est un homomorphisme de H dans G, on dit que G et H sont* isomorphes, *et on note $G \cong H$.*

Définition 1.4. *Soit G un graphe. Une* coloration *de G est une fonction $f : V(G) \to \mathbb{Z}^+$. On appelle* couleurs *les éléments de $Image(f)$. On dit que f est une* coloration propre *si pour toute arête $\{x, y\}$ de G les couleurs affectées à x et à y sont distinctes.*

Par la suite, nous utiliserons coloration pour parler d'une coloration propre. Le *nombre chromatique* d'un graphe G, noté $\chi(G)$, est le nombre minimum de couleurs nécessaires pour colorer les sommets de G, c'est-à-dire,

$$\chi(G) = \min_{f \in \mathcal{C}} \{ |Image(f)| \},$$

où $\mathcal{C} = \{f : f \text{ est une coloration de } G\}$.

Définition 1.5. *Soit G un graphe. La cardinalité du plus grand graphe complet qui est un sous-graphe de G est notée $\omega(G)$. Un graphe G est dit* faiblement γ-parfait *si $\chi(G) = \omega(G)$. Un graphe est dit* parfait *si tous ses sous-graphes induits sont faiblement γ-parfaits.*

Dans ce qui suit, il sera fréquent d'utiliser l'identification de deux sommets d'un graphe. Étant donné u et v deux sommets d'un graphe G, l'opération d'identification des sommets u et v consiste simplement à ajouter un nouveau sommet w adjacent à tous les sommets appartenant à $N(\{u, v\})$, le voisinage de $\{u, v\}$, et à enlever les sommets u et v.

Définition 1.6. *Un graphe G est dit* planaire *s'il peut être dessiné dans le plan de manière à ce qu'il n'y ait aucune intersection entre deux arêtes. Le dessin de G dans le plan satisfaisant cette condition est appelé* plongement de G dans le plan. *Étant donné un plongement de G dans le plan, un cycle C définit deux régions dans le plan, la région bornée par le cycle et la région non bornée. On appelle* face du graphe G *un cycle F avec la propriété que tous les sommets et toutes les arêtes de G n'appartenant pas à F se trouvent dans la même région (bornée ou non bornée) définie par F. Le nombre d'arêtes (ou de façon équivalente le nombre de sommets) de la face F est appelé* degré de la face F *et est noté* $\deg(F)$. *Une face est dite* paire *si elle est de degré pair et* impaire *si elle est de degré impair.*

1.3.2 Définitions sur les T-colorations

Les T-colorations ont été introduites par Hale (1980) pour modéliser le problème d'affectation de fréquences en théorie de la communication. Du fait de cette application importante en théorie de la communication, les T-colorations ont été largement étudiées. Nous présentons dans cette section les différentes définitions et notations inhérentes à ce sujet. Voici tout d'abord la définition d'une T-coloration.

Définition 1.7. *Soit T un ensemble fini d'entiers positifs ou nuls contenant* 0. *Un tel ensemble est aussi appelé* T-ensemble, *et s'il n'y a pas de confusion possible, nous utiliserons simplement "ensemble T". Une* T-coloration f *d'un graphe G est une coloration de G telle que pour toute arête $\{x, y\}$ de G, on a $|f(x) - f(y)| \notin T$.*

Pour déterminer l'efficacité d'une T-coloration, on peut considérer différents critères. Soit f une T-coloration d'un graphe G. Le nombre de couleurs utilisées par f pour T-colorer G est appelé l'*ordre* de f. On définit l'*étendue* de f comme étant le maximum de $\{|f(x) - f(y)| : x$ et y sont des sommets de $G\}$. L'*étendue-arête* de f est le maximum de $\{|f(x) - f(y)| : \{x, y\} \in E(G)\}$.

Définition 1.8. *Le* nombre T-chromatique *d'un graphe G, noté $\chi_T(G)$, est l'ordre minimal d'une T-coloration de G.*

Définition 1.9. *La* T-étendue d'un graphe G, *notée $sp_T(G)$, est l'étendue minimale d'une T-coloration de G.*

Définition 1.10. *La* T-étendue-arête *d'un graphe G, notée $esp_T(G)$, est l'étendue-arête minimale d'une T-coloration de G.*

On peut mesurer l'efficacité d'une T-coloration f d'un graphe G en comparant son ordre, son étendue et son étendue-arête à $\chi_T(G)$, à $sp_T(G)$ et à $esp_T(G)$, respectivement.

On définit la *T-étendue restreinte*, notée $rsp_T(G)$, comme étant l'étendue minimale d'une T-coloration qui utilise $\chi_T(G)$ couleurs. De même, on définit le *nombre T-chromatique restreint* d'un graphe G, noté $\chi_T^r(G)$, comme étant l'ordre minimal d'une T-coloration d'étendue $sp_T(G)$.

L'exemple suivant, illustré à la Figure 1.4, montre qu'il est possible, tel qu'indiqué par Hale (1980), qu'aucune T-coloration d'ordre optimal n'ait une étendue optimale, et vice versa.

Exemple 1.11. *Soit* $T = \{0, 1, 4, 5\}$ *et* C_5 *le cycle d'ordre 5. La Figure 1.4 illustre une* T*-coloration qui satisfait* $\chi_T^r(C_5) = 5$ *alors que* $sp_T(C_5) = 4$ *et une* T*-coloration satisfaisant* $rsp_T(C_5) = 6$ *alors que* $\chi_T(C_5) = \chi(C_5) = 3$.

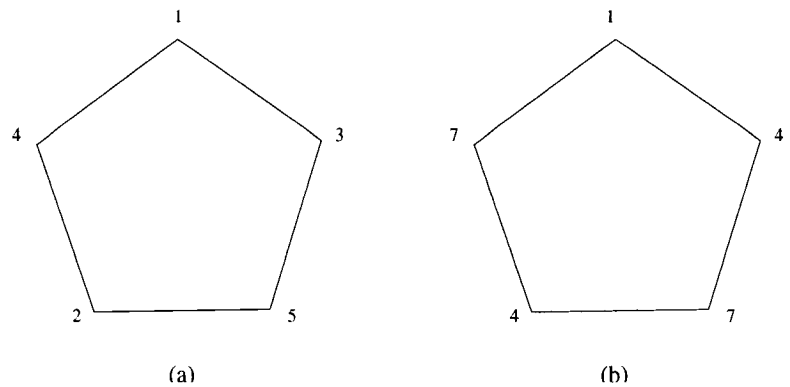

FIGURE 1.4 – *Une* T*-coloration avec* $\chi_T^r(C_5) = 5$ *pour* $sp_T(C_5) = 4$ *(a) et une* T*-coloration avec* $rsp_T(C_5) = 6$ *pour* $\chi_T(C_5) = 3$ *(b) avec* C_5 *et* $T = \{0, 1, 4, 5\}$.

1.3.3 Résultats généraux sur les T-colorations

Lorsqu'on s'intéresse à la résolution d'un problème, il est avantageux de savoir si ce problème est difficile, au sens de la théorie de la complexité. Nous présentons brièvement des résultats sur la NP-complétude des T-colorations. Nous poursuivons ensuite avec une énumération des résultats généraux concernant les T-colorations.

NP-complétude

Pour voir que le problème de T-coloration est NP-complet, il suffit de remarquer que lorsqu'on restreint l'ensemble T à $\{0\}$, le problème de $\{0\}$-coloration est en fait le problème de coloration usuel sur les graphes qui est lui-même NP-complet (Garey et Johnson, 1979) . Ainsi, la réduction du problème de coloration au problème de

T-coloration est immédiate et le problème de T-coloration est donc NP-complet, puisqu'on peut vérifier en temps polynomial qu'une T-coloration f satisfait les contraintes du problème.

Lorsqu'on sait qu'un problème est NP-complet, on s'intéresse généralement à des classes restreintes de ce problème. On veut de cette manière déterminer si certaines classes possèdent des méthodes de résolution plus rapides. Une des classes très importantes pour les T-colorations, comme nous le verrons un peu plus loin, est la classe des graphes complets. Gräf (1998) et Jansen (1996) ont montré indépendamment que le problème de T-coloration restreint aux graphes complets demeure NP-complet. Gräf utilise une réduction du problème de la clique au problème de T-coloration. De son côté, Jansen obtient une réduction du problème 3-SAT au problème de T-coloration. Le lecteur intéressé à la théorie de la complexité peut se référer à (Garey et Johnson, 1979).

Résultats de base sur les T-colorations

Bien que le problème de T-coloration soit un problème NP-complet, il est possible d'obtenir certains résultats sur le sujet en considérant quelques restrictions. Plus particulièrement, nous présentons des bornes pour l'étendue et l'étendue-arête des graphes. De plus, pour certaines classes de graphes, il est possible d'obtenir une réduction à un problème sur un graphe complet, d'où l'importance de l'étude des T-colorations sur les graphes complets. Il en est de même pour certains types d'ensembles T. D'autres résultats sur des types d'ensembles T et des classes de graphes particuliers seront présentés.

Premièrement, notons que pour tout graphe G et tout ensemble T, on a $\chi_T(G) = \chi(G)$ (Roberts, 1991*a*). En effet, puisqu'une T-coloration f est une coloration au sens usuel, on a $\chi_T(G) \geq \chi(G)$. De plus, puisque T est un ensemble fini, $max\ T$ existe ;

notons-le r. Ainsi, si toutes les différences $|f(x)-f(y)|$ sont supérieures à r (où $\{x,y\}$ est une arête de G), alors les contraintes de T-coloration seront respectées. Il suffit donc de prendre $\chi(G)$ nombres dont le premier est 1 et les suivants sont $r+2$, $2r+3$, $3r+4$, etc. On a bien une T-coloration f avec $\chi_T(G) = \chi(G)$. Ce raisonnement nous conduit donc aux bornes suivantes pour l'étendue d'un graphe G.

Proposition 1.12. *(Roberts, 1991a) Pour tout graphe G et ensemble T, on a*

$$\chi(G) - 1 \leq esp_T(G) \leq sp_T(G) \leq (r+1)(\chi(G)-1).$$

La borne supérieure a été améliorée par Tesman (1990) qui a prouvé que pour tout graphe G et tout ensemble T on a $sp_T(G) \leq |T|(\chi(G)-1)$. Notons également que s'il existe un homomorphisme h de G dans H alors $sp_T(G) \leq sp_T(H)$. En effet, soit f une T-coloration de H d'étendue $sp_T(H)$. Alors $f \circ h$ est une T-coloration de G d'étendue $sp_T(H)$, d'où $sp_T(G) \leq sp_T(H)$. On obtient donc la proposition suivante.

Proposition 1.13. *(Roberts, 1991a) Pour tout graphe G et tout ensemble T, on a*

$$sp_T(K_{\omega(G)}) \leq esp_T(G) \leq sp_T(G) \leq sp_T(K_{\chi(G)}).$$

Corollaire 1.14. *(Roberts, 1991a) Si G est faiblement γ-parfait, alors*

$$sp_T(G) = sp_T\left(K_{\chi(G)}\right).$$

Pour des ensembles T particuliers, définis ci-dessous, on peut déterminer l'étendue d'un graphe G par rapport à $\chi(G)$.

Définition 1.15. *a) Un ensemble T est appelé* ensemble r-initial *s'il est de la forme : $\{0,1,...,r\} \cup S$, où S ne contient aucun multiple de $r+1$.*
b) Un ensemble T est appelé ensemble k-multiples de s *s'il est de la forme : $\{0,s,2s,...,ks\} \cup S$, où $s \geq 1$, $k \geq 1$, et $S \subseteq \{s+1, s+2, ..., ks-1\}$.*

Proposition 1.16. *(Roberts, 1991a) a) Si T est r-initial alors pour tout graphe G, on a*

$$sp_T(G) = sp_T\left(K_{\chi(G)}\right) = (r+1)(\chi(G)-1).$$

b) Si T est k-multiples de s alors pour tout graphe G, on a

$$sp_T(G) = sp_T\left(K_{\chi(G)}\right) = \begin{cases} st + skt - sk - 1 & , si\ \chi(G) = st\,; \\ st + skt + m - 1 & , si\ \chi(G) = st + m, \\ & \quad pour\ un\ m\ tel\ que \\ & \quad 1 \leq m \leq s-1. \end{cases}$$

En ce qui concerne les résultats portant sur les graphes particuliers, on peut résumer la situation par la proposition suivante :

Proposition 1.17. *Soit H un sous-graphe de G. S'il existe un homomorphisme de G dans H, alors $sp_T(G) = sp_T(H)$ quel que soit l'ensemble T.*

Pour voir certaines conditions sur les graphes et les ensembles T auxquelles il est possible de trouver, en temps polynomial, l'étendue d'un graphe, le lecteur peut se référer à l'article de survol de Roberts (1991*b*). Dans cet article, on présente également des résultats concernant les T-listes-colorations, les T-ensembles-colorations et d'autres notions relatives aux T-colorations.

1.3.4 Résultats récents

En ce qui concerne les nouveaux développements sur le sujet des T-colorations, les résultats proviennent généralement de l'investigation de certaines classes de graphes et d'ensembles T particuliers. Nous présentons premièrement des résultats connus pour des graphes appelés puissances de cycles. Nous poursuivons avec un aperçu de la littérature concernant les T-graphes, qui sont étroitement liés aux graphes appelés graphes de distances. Nous présentons ensuite les résultats connus sur la T-étendue pour certains types d'ensembles T, ainsi qu'une généralisation des ensembles r-initiaux.

Graphes puissances de cycles

Les résultats suivants pour les puissances de cycles concernent la T-étendue-arête. Nous présentons les cas où la valeur exacte de la T-étendue-arête est connue et nous examinons ensuite des bornes pour les autres cas. Voici un résultat dû à Liu (1991) concernant les cycles d'ordre impair. Ce résultat sera par la suite vu comme cas particulier des graphes puissances de cycles.

Théorème 1.18. *Pour tout cycle d'ordre impair C_n et tout T de la forme $\{0, 1, ..., k-1\}$, on a*

$$esp_T(C_n) = \left\lceil \frac{(n+1)k}{n-1} \right\rceil.$$

Définition 1.19. *La d-ième* puissance du cycle C_n, *notée C_n^d, est définie comme*

$$V(C_n^d) = V(C_n) = \{v_0, v_1, ..., v_{n-1}\}, \text{ et}$$

$$E(C_n^d) = \bigcup_{0 \leq i \leq n-1} \{\{v_i, v_j\} : j = i+1, i+2, ..., i+d\},$$

où les sommes sont prises modulo n.

Notons d'abord que si $d \geq \lfloor n/2 \rfloor$, C_n^d est isomorphe à K_n. Dans ce qui suit, les résultats font référence à $T = \{0, 1, ..., k-1\}$. Par conséquent, si $d \geq \lfloor n/2 \rfloor$, on a que $esp_T(C_n^d) = sp_T(K_n) = k(n-1)$. Ainsi, par la suite, on se restreint aux $d \leq \lfloor n/2 \rfloor - 1$, et on note $n = m(d+1) + r$, où $m \geq 2$ et $0 \leq r \leq d$. Voici maintenant les principaux résultats sur les puissances de cycles (Hu et al., 1999).

Théorème 1.20. *Soit $n = m(d+1) + r$, pour $m \geq 2$, $0 \leq r \leq d$, et soit $T = \{0, 1, ..., k-1\}$. Alors*

$$dk \leq esp_T(C_n^d) \leq sp_T(C_n^d) = dk + \lceil r/m \rceil k.$$

Pour le cas particulier où $r = 0$, on obtient le corollaire suivant :

Corollaire 1.21. *Soient* $n = m(d+1)$ *et* $T = \{0, 1, ..., k-1\}$. *Alors*

$$esp_T(C_n^d) = sp_T(C_n^d) = dk.$$

Pour le cas particulier où n et $d+1$ sont relativement premier, il est possible d'obtenir une meilleure borne supérieure. On peut également obtenir une meilleure borne inférieure dans le cas où $r \geq 1$. Ces deux cas sont résumés dans le théorème suivant.

Théorème 1.22. *Soit* $n = m(d+1) + r$, *pour* $m \geq 2$, $0 \leq r < d$, *et soit* $T = \{0, 1, ..., k-1\}$.
a) Si $pgcd(n, d+1) = 1$ *alors* $esp_T(C_n^d)$ *est au plus* $dk + \lceil rk/m \rceil$.
b) Si $1 \leq r \leq d$ *alors* $esp_T(C_n^d)$ *est au moins* $dk + \lceil k/m \rceil$.

On obtient de ce théorème la valeur exacte pour le cas $r = 1$, puisque si $n = m(d+1) + 1$ alors $pgcd(n, d+1) = 1$.

Corollaire 1.23. *Si* $r = 1$, *alors* $esp_T(C_n^d) = dk + \lceil k/m \rceil$.

Il est intéressant de noter que le théorème 1.18 est le cas particulier pour $d = 1$ de ce corollaire. De plus, si $n \geq 5$ est impair et que $d = \frac{n-3}{2}$, alors r est égal à 1, m est égal à 2, et C_n^d est isomorphe à $\overline{C_n}$. On obtient ainsi le résultat suivant.

Corollaire 1.24. *Si* $n \geq 5$ *est impair, alors* $esp_T(\overline{C_n}) = \lceil (n-2)k/2 \rceil$.

1.3.5 T-graphes

La notion de T-graphe a été introduite par Liu (1992). Les T-graphes forment une famille de graphes qui s'avère un outil efficace pour l'étude des T-colorations. Nous présentons ici les différents résultats concernant les T-graphes.

Définition 1.25. *Soit T un ensemble d'entiers positifs ou nuls incluant 0. Le* T-graphe, *noté G_T, est défini par $V(G_T) = \mathbb{Z}^+$ et $\{x, y\} \in E(G_T)$ si et seulement si $|x - y| \notin T$. Le* T-graphe d'ordre n, *noté G_T^n, est le sous graphe de G_T induit par $\{0, 1, ..., n-1\}$.*

Notons que par définition de G_T, la numérotation des sommets induit une T-coloration de G_T^n. Ainsi, $sp_T(G_T^n) \leq n - 1$, pour tout n. Voici quelques propriétés supplémentaires provenant d'un article de Liu (1992) :

(a) $sp_T(G)$ est inférieur ou égal à $n - 1$ si et seulement si G est homomorphe à G_T^n.

(b) Si n est le minimum tel que $\chi(G_T^n) \geq \chi(G)$ alors $sp_T(G)$ est supérieur ou égal à $n - 1$.

(c) Si $sp_T(G)$ est inférieur à n alors $\chi(G_T^n)$ est supérieur ou égal à $\chi(G)$.

(d) Si $\omega(G_T^n)$ est supérieur ou égal à $\chi(G)$ alors $sp_T(G)$ est inférieur ou égal à $n - 1$.

Théorème 1.26. *(Liu, 1992) Étant donné T, les énoncés suivants sont équivalents :*
(i) $sp_T(G) = sp_T\left(K_{\chi(G)}\right)$ pour tout graphe G,
(ii) G_T^n est faiblement γ-parfait pour tout n.

De ce théorème, on tire différentes familles d'ensembles T pour lesquelles on a $sp_T(G) = sp_T\left(K_{\chi(G)}\right)$ pour tout G. En particulier, on montre d'une nouvelle manière que les ensembles r-initiaux et k-multiples de s satisfont cette propriété. D'autres familles la possèdent aussi. Pour plus de détails le lecteur peut se référer à l'article de Liu (1992).

La propriété $sp_T(G) = sp_T\left(K_{\chi(G)}\right)$ pour tout G est très forte pour un ensemble T. Le théorème suivant considère une relaxation de cette propriété, c'est-à-dire qu'on

veut que $sp_T(G) = sp_T(K_{\chi(G)})$ pour les graphes avec $\chi(G)$ fixé, plutôt que pour tous les graphes.

Théorème 1.27. *(Liu, 1992) Pour tout graphe G avec $\chi(G) = m$, on a $sp_T(G) = sp_T(K_m) = n - 1$ si et seulement si $\omega(G_T^n) = \chi(G_T^n) = m$ et $\chi(G_T^{n-1}) < \chi(G_T^n)$.*

Ce théorème nous fournit une procédure qui permet de vérifier si $sp_T(G) = sp_T(K_m)$ pour les graphes avec $\chi(G) = m$. En effet, il suffit de trouver le plus petit n tel que $\omega(G_T^n) = m$. Ensuite, on vérifie si $\omega(G_T^n) = \chi(G_T^n)$ et $\chi(G_T^{n-1}) < \chi(G_T^n)$. Si cela est vrai, la propriété est vérifiée, sinon on peut trouver un contre-exemple en considérant G_T^n.

Les concepts qui suivent sont utiles à la présentation des prochains résultats. Tout d'abord, étant donné T, le T-algorithme glouton sur K_n est un algorithme qui colore les sommets de K_n de façon séquentielle, c'est-à-dire qu'à chaque étape on utilise la plus petite couleur qui respecte les contraintes de T-coloration. Nous noterons $\mathcal{G}$ la collection des ensembles T pour lesquels le T-algorithme glouton donne la T-étendue optimale de K_n, pour tout $n \geq 1$. Puis nous noterons $\mathcal{E}$ la collection des ensembles T pour lesquels $sp_T(G) = sp_T\left(K_{\chi(G)}\right)$ pour tout graphe G.

Définition 1.28. *Le* produit disjoint *de n graphes, noté $G = G_1 \times G_2 \times \cdots \times G_n$, est défini par $V(G) = V(G_1) \sqcup V(G_2) \sqcup \cdots \sqcup V(G_n)$, où $\sqcup$ représente l'union disjointe. De plus, $\{u, v\} \in E(G)$ si et seulement si $\{u, v\} \in E(G_i)$ pour un i, ou bien $u \in V(G_i)$ et $v \in V(G_j)$, $i \neq j$.*

Étant donné T un ensemble d'entiers et $a \in \mathbb{Z}^+$, nous noterons $aT = \{at : t \in T\}$. Voici les principaux résultats concernant les ensembles de la forme aT (Liu, 1996).

Théorème 1.29. *Pour tout T et $a \in \mathbb{Z}^+$, notons G^i, le sous-graphe du T-graphe G_{aT} induit par les sommets $\{ka + i : k \in \mathbb{Z}^+\}$, $0 \leq i \leq a - 1$. Alors $G_{aT} = G^0 \times G^1 \times \cdots \times G^{a-1}$ et $G^i \cong G_T$, pour $0 \leq i \leq a - 1$.*

Théorème 1.30. *$T \in \mathcal{E}$ si et seulement si $aT \in \mathcal{E}$ pour tout $a \in \mathbb{Z}^+$.*

Théorème 1.31. *$T \in \mathcal{G}$ si et seulement si $aT \in \mathcal{G}$ pour tout $a \in \mathbb{Z}^+$.*

Le prochain théorème nous donne un type d'ensembles T tels que $T \in \mathcal{G}$ et une condition nécessaire et suffisante pour que T appartienne à $\mathcal{E}$. En particulier, ce type d'ensembles est une généralisation des ensembles r-initiaux et k-multiples de s.

Théorème 1.32. *Soit $T = \{0, as, a(s+1), ..., a\ell\} \cup A$, où $a \in \mathbb{Z}^+$ et $A \subseteq \{as + 1, as + 2, ..., a\ell - 1\}$. Alors,*
(i) $T \in \mathcal{G}$, et
(ii) $T \in \mathcal{E}$ si et seulement si $\ell = ms$, pour un $m \in \mathbb{Z}^+$.

Divisibilité et T-étendue

Dans cette partie, nous étudions la T-étendue des graphes pour de nouveaux types d'ensembles T, soient T/d, T_d, $d \odot T$, ainsi que l'ensemble dT, défini à la partie précédente (Janczewski, 2001).

Définition 1.33. *Soit T un ensemble, $T^c = \{0, 1, ..., \max T + 1\} - T$, et soit d un entier strictement positif. On définit*
(a) $dT = \{dt | t \in T\}$,
(b) $T/d = \{t | dt \in T\}$,
(c) $T_d = \{0, 1, 2, ..., \lceil (\max T + 1)/d \rceil\} - \{\lfloor t/d \rfloor, \lceil t/d \rceil | t \in T^c\}$, et
(d) $d \odot T = \{0, 1, 2, ..., d(\max T + 1)\} - dT^c$.

Proposition 1.34. *(Janczewski, 2001) Soit d un entier strictement positif. Alors (i) $sp_T(G) \leq d \cdot sp_{T/d}(G)$ et (ii) $sp_{dT}(G) \leq d \cdot sp_T(G)$.*

Proposition 1.35. *(Janczewski, 2001) Soit d un entier strictement positif satisfaisant $d \leq \min T^c$. Alors $sp_T(G) \geq d \cdot sp_{T_d}(G)$.*

Soit d un entier strictement positif satisfaisant $d \leq \min T^c$. En combinant les deux propositions précédentes on a des bornes pour la T-étendue d'un graphe G. Autrement dit, on a $d \cdot sp_{T_d}(G) \leq sp_T(G) \leq d \cdot sp_{T/d}(G)$. Il est donc intéressant d'étudier les cas où $T/d = T_d$, puisque dans ces cas on obtient une égalité à la place des bornes. Le théorème suivant nous donne une condition suffisante pour que $T/d = T_d$.

Théorème 1.36. *(Janczewski, 2001) Si d est un entier strictement positif qui divise tous les éléments de l'ensemble T^c, alors*
(i) $T/d = T_d$ et (ii) $sp_T(G) = d \cdot sp_{T/d}(G)$.

Voici maintenant un résultat concernant les ensembles de la forme $d \odot T$.

Théorème 1.37. *(Janczewski, 2001) Soit d un entier strictement positif. Alors*
(i) $(d \odot T)/d = T$ et (ii) $sp_{d\odot T}(G) = d \cdot sp_T(G)$

Nous présentons maintenant une généralisation des ensembles r-initiaux, appelée ensembles (r, T)-initiaux. Nous montrons ensuite sous quelles conditions ces ensembles appartiennent à $\mathcal{E}$ et à $\mathcal{G}$.

Définition 1.38. *Soit $r \in \mathbb{Z}^+$ et soit T un ensemble. Un ensemble fini $S \subseteq \mathbb{Z}^+$ est dit* (r, T)-initial *si et seulement si $(r+1) \odot T \subseteq S$ et $S/(r+1) = T$.*

On remarque qu'un ensemble r-initial est $(r, \{0\})$-initial et que tout ensemble T est $(0, T)$-initial.

Proposition 1.39. *(Janczewski, 2001) Soit S un ensemble (r, T)-initial et G un graphe. Alors $sp_S(G) = (r+1) \cdot sp_T(G)$.*

Théorème 1.40. *(Janczewski, 2001) Soit S un ensemble (r, T)-initial. Alors*
(i) $S \in \mathcal{E} \Leftrightarrow T \in \mathcal{E}$ et (ii) $S \in \mathcal{G} \Leftrightarrow T \in \mathcal{G}$.

Comme on peut le constater, les résultats obtenus pour les T-colorations sont tous relatifs à la forme de l'ensemble T et quelquefois à la forme du graphe qui doit être T-coloré. Nous présentons à la fin de ce chapitre des résultats que nous avons obtenus pour différentes classes de graphes et qui ont la particularité d'être des algorithmes indépendants de la structure de l'ensemble T.

1.4 Homomorphismes de graphes

1.4.1 Préliminaires

Pour une utilité future, nous présentons maintenant une autre définition d'homomorphisme de graphes. Cette définition, qui est équivalente à la définition précédente d'homomorphisme, nous donne une autre perception de cette notion en nous permettant de décomposer un homomorphisme en plusieurs homomorphismes élémentaires.

Définition 1.41. *(Harary, 1969) Un* homomorphisme élémentaire *d'un graphe G est une identification de deux sommets non adjacents de G. On appelle* image homomorphique *de G n'importe quelle séquence d'homomorphismes élémentaires de G. Soit $f(G)$ une image homomorphique de G. Lorsque $f(G)$ est un sous-graphe de H on dit que G est* homomorphe *à H, ce que l'on note $G \rightarrow H$, comme pour la définition 1.3.*

Remarque 1.42. *La définition d'homomorphisme de G dans H implique qu'un homomorphisme n'est pas toujours surjectif. Par exemple, tout sous-graphe propre de G a un homomorphisme dans G.*

L'exemple suivant nous montre les images homomorphiques d'un graphe particulier.

Exemple 1.43. *Le chemin d'ordre 4, noté P_4, possède seulement les quatre images homomorphiques qui sont illustrées à la Figure 1.5.*

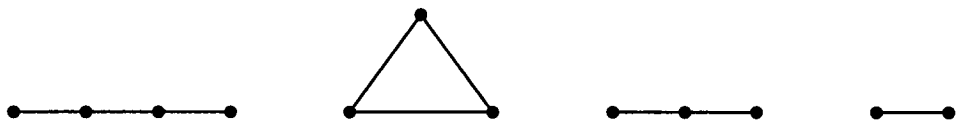

FIGURE 1.5 – *Images homomorphiques de P_4.*

Une H-coloration de G est simplement un homomorphisme de G dans H. On note alors qu'une coloration de G avec q couleurs, au sens usuel, est en fait une K_q-coloration de G, c'est-à-dire un homomorphisme de G dans K_q. Ainsi, la notion de H-coloration généralise bien la notion de coloration usuelle. De plus, on remarque qu'une T-coloration s'exprime en termes de H-coloration, où $V(H)$ est un ensemble d'entiers et pour tous $x, y \in V(H)$, $x \neq y$, on a $\{x, y\} \in E(H) \Leftrightarrow |x - y| \notin T$. La notion de H-coloration généralise donc également la notion de T-coloration.

Le problème de la H-coloration consiste à déterminer si un graphe possède une H-coloration. Si H est biparti, le problème de H-coloration appartient à la classe des problèmes polynomiaux. Toutefois, Hell et Nesětril (1986) ont montré que pour tout graphe H non biparti, le problème de H-coloration appartient à la classe des problèmes NP-complets.

1.4.2 Résultats généraux sur les homomorphismes

Le résultat suivant, dû à Harary et al. (1967), indique l'effet d'un homomorphisme élémentaire sur le nombre chromatique d'un graphe.

Théorème 1.44. *Soit G un graphe. Pour tout homomorphisme élémentaire ϵ de G, on a*

$$\chi(G) \leq \chi(\epsilon(G)) \leq \chi(G) + 1.$$

Preuve. Soit ϵ l'homomorphisme élémentaire de G qui identifie les sommets non adjacents u et v de G. Alors une coloration de $\epsilon(G)$ induit une coloration de G en

prenant pour couleur de u et v la couleur du sommet issu de leur identification dans $\epsilon(G)$. Donc, $\chi(G) \leq \chi(\epsilon(G))$. D'autre part, en partant d'une coloration de G, on construit une coloration de $\epsilon(G)$ en colorant le sommet issu de l'identification de u et v d'une nouvelle couleur, d'où $\chi(\epsilon(G)) \leq \chi(G) + 1$.

□

Corollaire 1.45. *(Hajós, 1961) Pour tout homomorphisme f de G, on a*

$$\chi(G) \leq \chi(f(G)).$$

Puisque le nombre T-chromatique d'un graphe G est égal à son nombre chromatique, les résultats précédents s'appliquent également à $\chi_T(G)$. Autrement dit, quels que soient G et T, on a $\chi_T(G) \leq \chi_T(\epsilon(G)) \leq \chi_T(G) + 1$ pour tout homomorphisme élémentaire ϵ. De même, pour tout homomorphisme f de G, on a $\chi_T(G) \leq \chi_T(f(G))$.

En ce qui concerne la T-étendue d'un graphe G, nous obtenons des résultats analogues.

Théorème 1.46. *Soit G un graphe et T un ensemble d'entiers. Notons $\tau(T, G) = max\, T + sp_T(G) + 1$. Alors pour tout homomorphisme élémentaire ϵ de G, on a*

$$sp_T(G) \leq sp_T(\epsilon(G)) \leq sp_T(G) + \tau(T, G).$$

Preuve. Soit ϵ l'homomorphisme élémentaire de G qui identifie les sommets non adjacents u et v de G. Alors une T-coloration de $\epsilon(G)$ induit une T-coloration de G en prenant pour couleur de u et v la couleur que le sommet identifié avait dans $\epsilon(G)$. Donc, $sp_T(G) \leq sp_T(\epsilon(G))$. D'autre part, en partant d'une T-coloration de G, on construit une T-coloration de $\epsilon(G)$ en colorant le sommet issu de l'identification de u et v avec la couleur $\tau(T, G)$. Puisqu'aucune distance générée par ce nouveau sommet n'est inférieure à $\max T$, on a nécessairement une T-coloration, d'où $sp_T(\epsilon(G)) \leq sp_T(G) + \tau(T, G)$.

□

Corollaire 1.47. *Pour tout homomorphisme f de G, quel que soit l'ensemble T, on a la propriété suivante*

$$sp_T(G) \leq sp_T(f(G)).$$

Corollaire 1.48. *Soit f un homomorphisme de G. Si $f(G)$ est un sous-graphe de G alors on a*

$$sp_T(G) = sp_T(f(G)).$$

Preuve. En effet, puisque $f(G)$ est un sous-graphe de G on a $sp_T(f(G)) \leq sp_T(G)$ et le corollaire 1.47 termine la preuve.

□

Rappelons qu'un graphe G est dit faiblement γ-parfait si $\chi(G) = \omega(G)$, c'est-à-dire si son nombre chromatique est égal à l'ordre d'une clique maximale de G.

Corollaire 1.49. *Si G est faiblement γ-parfait alors quel que soit l'ensemble T, on a*

$$sp_T(G) = sp_T\left(K_{\chi(G)}\right).$$

Preuve. Puisque G est faiblement γ-parfait, $K_{\chi(G)}$ est un sous-graphe de G et G est homomorphe à $K_{\chi(G)}$. Le corollaire 1.48 termine la preuve.

□

1.4.3 Cores et T-colorations

Un homomorphisme du graphe H vers le graphe G est noté $H \to G$. Notons

$$H \leftrightarrow G$$

si $H \to G$ et $G \to H$. La relation $\leftrightarrow$ est une relation d'équivalence. Soit $\mathcal{C}$ une classe d'équivalence de $\leftrightarrow$. Soit X et Y deux graphes de $\mathcal{C}$ ayant un nombre minimum de sommets. Comme $X \leftrightarrow Y$, il existe un homomorphisme f de X vers Y. Si

$$|V(f(X))| < |V(X)|,$$

la minimalité de $|V(Y)|$ est violée ; f doit donc être surjectif. f est donc un isomorphisme et l'on conclut qu'il existe, à isomorphisme près, un unique graphe dans $\mathcal{C}$ ayant un nombre minimum de sommets. On dit que ce graphe est un *core*, et le choix de ce graphe comme représentant de sa classe d'équivalence est naturel.

Remarque 1.50. *Si X est un core et que f est un homomorphisme de X vers X, alors f est un automorphisme. L'inverse est aussi vrai, et cette propriété est habituellement utilisée comme définition de core (Hell et Nešetřil, 2004).*

Soit H un graphe dans la classe $\mathcal{C}$. Alors le core de la classe $\mathcal{C}$ est un sous-graphe induit de H. On l'appelle le *core de H*, et on le note $H^\bullet$.

Exemple 1.51. *(Hell et Nešetřil, 2004) Les graphes suivants sont des cores :*

1. *les graphes complets ;*
2. *les cycles impairs ;*
3. *les roues d'ordre pair ;*
4. *le graphe de Petersen.*

Si f est un homomorphisme de H vers G et que $\varphi : V(G) \to \mathbb{Z}$ est une T-coloration pour un ensemble T donné, alors $\varphi \circ f$ est une T-coloration de H. On en déduit que $sp_T(H) \leq sp_T(G)$. Ainsi, si $H \leftrightarrow G$, alors

$$sp_T(H) = sp_T(G),$$

et une T-coloration de H induit une T-coloration de G et vice versa. Par conséquent, le problème de T-coloration se réduit au problème de T-coloration des cores.

Exemple 1.52. *Si H est biparti, alors $H^\bullet \cong K_2$; le problème de T-coloration des graphes bipartis est trivial.*

On a vu plus haut, esquissée, la preuve de la proposition suivante.

Proposition 1.53. *Pour tout graphe H et pour tout $T \subset \mathbb{Z}_+$,*

$$sp_T(H) = sp_T(H^\bullet).$$

Remarque 1.54. *La proposition 1.53 est équivalente au corollaire 1.48, le résultat est répété simplement pour illustrer la notion de core et son utilité.*

1.5 Algorithmes et résultats

Dans cette section nous proposons de déterminer des classes de graphes pour lesquels il est possible de trouver la T-étendue de manière efficace. Pour ce faire, nous utilisons les notions d'homomorphisme, de core et de T-graphe vues précédement.

1.5.1 La classe des cycles impairs

Dans cette partie, nous proposons un algorithme exact pour déterminer la T-étendue des cycles impairs. Cet algorithme utilise la notion de T-graphes et les différents résultats déjà vus concernant les homomorphismes.

Notons d'abord que pour C et C' deux cycles impairs tels que $|C| < |C'|$, on a $sp_T(C') \leq sp_T(C)$, puisqu'il existe un homomorphisme de C' dans C. Pour vérifier cette affirmation, il suffit de montrer que pour tout entier $m \geq 1$ il existe un homomorphisme de C_{2m+3} dans C_{2m+1}. En effet, si $|C| < |C'|$ alors il existe une suite de cycles impairs $\{C_i\}_{i=0}^n$ telle que $|C_0| = |C|$, $|C_n| = |C'|$ et telle que pour tout

$i = 0, 1, \ldots n-1$ on ait $|C_i| + 2 = |C_{i+1}|$. Montrons donc que $C_{2m+3} \rightarrow C_{2m+1}$. En effet, si x_1, x_2, x_3 et x_4 sont quatre sommets consécutifs dans C_{2m+3}, de tels sommets existent toujours puisque $m \geq 1 \Rightarrow |C_{2m+3}| \geq 5$, alors en identifiant les sommets x_1 et x_3 puis les sommets x_2 et x_4 on obtient ainsi un graphe isomorphe à C_{2m+1}. Par conséquent, C_{2m+3} est bien homomorphe à C_{2m+1}. Ce qui prouve bien l'affirmation initiale.

Définition 1.55. *La* maille *d'un graphe G est l'ordre du plus petit cycle qui est un sous-graphe induit de G. La* maille impaire *de G est l'ordre du plus petit cycle impair qui est un sous-graphe induit de G.*

Lemme 1.56. *Le cycle d'ordre $2k+1$ est homomorphe à un graphe G si et seulement G contient un sous-graphe isomorphe à un cycle impair d'ordre au plus $2k+1$.*

Preuve. Il est évident que si G contient un cycle impair d'ordre au plus $2k+1$ alors $C_{2k+1} \rightarrow G$.

Montrons donc que $C_{2k+1} \rightarrow G$ implique que G contient un cycle impair d'ordre au plus $2k+1$. Procédons par récurrence. Si $k = 1$ alors $C_{2k+1} = K_3$ le graphe complet sur 3 sommets. G doit nécessairement contenir un sous-graphe isomorphe à K_3 puisqu'aucun homomorphisme élémentaire n'est possible sur K_3. La propriété est donc vraie pour $k = 1$. Supposons la propriété vraie pour $k \geq 1$ et vérifions-la pour $k+1$. Étant donné le cycle d'ordre C_{2k+3}, de n'importe quel homomorphisme élémentaire de ce cycle on obtient une image homomorphique de C_{2k+3} qui contient un cycle impair d'ordre au plus $2k+1$. Tous les graphes obtenus de C_{2k+3} par un homomorphisme élémentaire sont, par hypothèse de récurrence, homomorphes à des graphes contenant un cycle impair d'ordre au plus $2k+1$. La seule image homorphique de C_{2k+3} qui ne contient pas un cycle impair d'ordre au plus $2k+1$ est C_{2k+3} lui-même. Ainsi, toutes les images homomorphiques de C_{2k+3} contiennent un cycle impair d'ordre au plus $2k+3$. Si $C_{2k+3} \rightarrow G$ alors G contient un sous-graphe isomorphe à une

image homomorphique de C_{2k+3} et par conséquent il contient donc un sous-graphe qui est un cycle impair d'ordre au plus $2k+3$. Par le principe de récurrence le lemme est démontré.

□

Étant donné G_T^{n+1}, le T-graphe d'ordre $n+1$, nous noterons d_{imp}^n la longueur du plus court chemin d'ordre impair allant du sommet 0 au sommet n, et d_{pair}^n la longueur du plus court chemin d'ordre pair allant du sommet 0 au sommet n.

Pour trouver la valeur de d_{imp}^n et de d_{pair}^n il suffit de considérer les voisinages successifs du sommet 0 jusqu'à ce qu'on ait atteint le sommet n (à faire pour le cas pair et pour le cas impair) ou qu'après avoir considéré le n-ième voisinage de 0 il n'existe pas de chemin d'ordre impair allant de 0 à k, auquel cas nous noterons $d_{imp}^n = \infty$, ou encore s'il n'existe pas de chemin d'ordre pair allant de 0 à k, nous noterons également $d_{pair}^n = \infty$.

Avant de donner l'algorithme pour T-colorer les cycles impairs, il est important de remarquer qu'il existe toujours un T-graphe d'ordre non-nul qui est biparti. En effet, il est évident que le T-graphe d'ordre 2 est biparti puisqu'il s'agit d'un graphe simple d'ordre deux. Il existe donc un plus grand entier $n \geq 2$ tel que G_T^n soit biparti. L'idée de l'algorithme est donc de considérer successivement les T-graphes à partir de celui d'ordre $sp_T(K_3)$ jusqu'à celui d'ordre $n+1$. Pour $i = sp_T(K_3), sp_T(K_3)-1, \ldots, n+1$ on associe alors à G_T^i la valeur $L_i = d_{imp}^i + d_{pair}^i$. De cette manière on peut obtenir la T-étendue pour tous les cycles impairs. L'algorithme 1.1, présenté ci-dessous, prend en entrée un T-ensemble et l'ordre d'un cycle impair et retourne la T-étendue pour ce cycle.

Proposition 1.57. *Étant donné un T-ensemble et un cycle impair d'ordre $2k+1$ l'algorithme 1.1 retourne bien la T-étendue du cycle C_{2k+1}.*

Algorithme 1.1 T-étendue d'un cycle impair d'ordre $2k+1$

Antécédent: un T-ensemble et un entier impair $2k+1$
Conséquent: la T-étendue de C_{2k+1}

1: **pour** $i = sp_T(K_3)$ **à** $n+1$ **faire**
2: Construire G_T^i
3: $L_i = d_{imp}^i + d_{pair}^i$
4: **si** $L_i \leq 2k+1$ **alors**
5: reponse $= i$
6: **fin si**
7: **fin pour**
8: **retourner** (reponse)

Preuve. En effet, puisque pour tout entier $k \geq 1$ on a $C_{2k+1} \rightarrow K_3$ alors $sp_T(K_3)$ est bien une borne supérieure pour la T-étendue de n'importe quel cycle impair. Comme on l'a déjà mentionné, il existe un entier $n \geq 1$ tel que G_T^n est biparti et G_T^{n+1} est non biparti. Ainsi, la T-étendue de n'importe quel cycle impair se situe bien entre $n+1$ et $sp_T(K_3)$.

Regardons maintenant ce que signifie la valeur de L_i. Premièrement, lorsque $L_i = \infty$ alors cela signifie que tous les chemins allant de 0 à i sont de même parité. Or, G_T^i n'est pas biparti puisque $i > n$. Donc G_T^i contient un cycle impair mais aucun cycle impair ne passe par les sommets 0 et i. Ainsi, pour n'importe quel cycle impair de G_T^i, il existe un cycle impair du même ordre dans G_T^{i-1}. Par conséquent, la T-étendue de n'importe quel cycle impair qui est un sous-graphe de G_T^i est strictement inférieure à i.

Deuxièmement, si $L_i \leq 2k+1$ on a alors $sp_T(C_{2k+1}) \leq i$ puisqu'il existe un homomorphisme entre C_{2k+1} et n'importe quelle paire de chemins allant d'un sommet u à un sommet v dont la somme des longueurs est inférieure à $2k+1$. En effet, si les chemins s'intersectent alors ils forment un cycle impair d'ordre inférieur à L_i, sinon ils forment le cycle d'ordre L_i ; dans les deux cas il existe bien un homomorphisme.

Soit m le plus petit entier tel que $L_m \leq 2k+1$. Supposons que $sp_T(C_{2k+1}) = i$,

avec $n < i < m$. Par définition du T-graphe d'ordre i, on a $C_{2k+1} \rightarrow G_T^i$. Le lemme 1.56 implique que G_T^i contient un cycle impair d'ordre au plus $2k+1$. Soit C un tel cycle. Notons a le plus petit entier qui est un sommet de C et notons b le plus grand entier qui est un sommet de C. Si $a \neq 0$ ou $b \neq i$ alors $sp_T(C_{2k+1}) \leq b - a < i$ ce qui contredit $sp_T(C_{2k+1}) = i$. Si $a = 0$ et $b = i$ alors $L_i \leq 2k+1$, ce qui contredit la définition de m puisque $i < m$. Ainsi, si m est le plus petit entier tel que $L_m \leq 2k+1$ alors $sp_T(C_{2k+1}) \geq m$.

Puisque d'une part on a $L_i \leq 2k+1 \Rightarrow sp_T(C_{2k+1}) \leq i$ et d'autre part on a que si m est le plus petit entier tel que $L_m \leq 2k+1$ alors $sp_T(C_{2k+1}) \geq m$. La T-étendue du cycle d'ordre $2k+1$ est nécessairement le plus petit entier m tel que $L_m \leq 2k+1$, c'est-à-dire, l'entier retourné par l'algorithme 1.1.

□

Proposition 1.58. *Étant donné un T-ensemble et un cycle impair d'ordre $2k+1$, l'algorithme 1.1 se termine en temps polynomial par rapport à $|T|$.*

Preuve. Le nombre d'itérations requises par l'algorithme 1.1 est borné par $sp_T(K_3)$. Or, un résultat, prouvé par Tesman (1989), affirme que

$$sp_T(G) \leq |T|(\chi(G) - 1).$$

Ce résultat implique que $sp_T(K_3) \leq 2|T|$, et donc que le nombre d'itérations est borné linéairement par rapport à $|T|$.

Pour chaque itération on construit le T-graphe d'ordre i, ceci se fait en temps polynomial puisque pour chaque paire de sommets il suffit de vérifier si la différence appartient à l'ensemble T. En fait, on peut seulement construire $G_T^{sp_T(K_3)}$ à la première itération, puis simplement ôter le dernier sommet aux itérations successives. Ceci ce fait dans l'ordre de $|T|^2$, ce qui est l'ordre du nombre d'arêtes maximum de $G_T^{sp_T(K_3)}$.

Pour chaque itération on trouve L_i, ceci se fait en temps polynomial puisqu'il suffit de considérer au plus i fois les voisinages d'un ensemble de sommets sur un graphe d'ordre i avec $i < 2|T|$. Ceci ce fait dans l'ordre de $|T|^2$, puisque chaque sommet à un nombre de voisins dans l'ordre de $|T|$.

Pour chaque itération on compare deux entiers ce qui se fait évidemment en temps constant.

Puisqu'on a $\mathcal{O}(|T|)$ itérations avec au plus $\mathcal{O}(|T|^2)$ opérations par itération, alors l'algorithme appartient à $\mathcal{O}(|T|^3)$ et il s'agit bien d'un algorithme polynomial.

□

1.5.2 La classe des roues

Comme nous le verrons, le cas des roues impaires est équivalent à la T-coloration de K_3, il est donc suffisant de restreindre notre étude au cas des roues paires. Dans cette partie, nous proposons donc un algorithme pour déterminer la T-étendue des roues paires. Cet algorithme utilise, comme pour les cycles impairs, la notion de T-graphes et les différents résultats déjà vus concernant les homomorphismes. Comme point de départ pour notre algorithme, il nous faut déterminer la T-étendue de K_4, qui est la plus petite roue paire, un algorithme sera donné à cet effet. Donnons d'abord la définition d'une roue.

Définition 1.59. *Une* roue *d'ordre $n \geq 4$, notée R_n, est définie par*

$$V(R_n) = \{1, 2, ..., n\}, \text{ et}$$

$$E(R_n) = \{\{i, n\} \mid 1 \leq i \leq n-1\} \bigcup \{\{i, i+1\} \mid 1 \leq i \leq n-2\} \bigcup \{\{n-1, 1\}\}.$$

Si n est un entier pair on dit que R_n est une roue paire *et si n est impair on dit que R_n est une roue impaire.*

Une roue paire est donc constituée d'un sommet central, adjacent à tous les sommets d'un cycle impair. De même, une roue impaire est constituée d'un sommet central adjacent à tous les sommets d'un cycle pair. Certains auteurs utilisent la notation R_n pour désigner une roue constituée d'un sommet central adjacent à tous les sommets d'un cycle d'ordre n c'est-à-dire, constituée de $n+1$ sommets.

Remarquons que R_4 est isomorphe à K_4. On peut aussi voir que si n est impair alors $\omega(R_n) = \chi(R_n) = 3$. Dans ce cas, par le corollaire 1.14, trouver une T-coloration de R_n d'étendue optimale, pour tout n impair, revient donc à trouver une T-coloration de K_3 d'étendue optimale. Puisque nous avons déjà résolu le cas de T-colorer K_3, nous considérerons, à partir de maintenant, que le cas des roues d'ordre impair. Voici d'abord un algorithme pour trouver la T-étendue de K_4. Rappelons que $N(0)$, qui est considérer par l'algorithme, est le voisinage du sommet 0 et donc un ensemble de sommets.

Algorithme 1.2 T-étendue de K_4

Antécédent: un T-ensemble
Conséquent: la T-étendue de K_4

1: **pour** $i = 3|T|$ **à** 4 **faire**
2: Construire G_T^i
3: **si** $i \in N(0)$ **alors**
4: **pour tout** $\{v_1, v_2\} \subseteq N(0)$ **faire**
5: **si** $\{i, v_1, v_2\}$ est un triangle **alors**
6: `reponse` $= i$
7: Sortir de la boucle
8: **fin si**
9: **fin pour**
10: **fin si**
11: **fin pour**
12: **retourner** (`reponse`)

Proposition 1.60. *Étant donné un T-ensemble l'algorithme 1.2 se termine en temps polynomial par rapport à $|T|$ en retournant $sp_T(K_4)$.*

Preuve. Tout d'abord, l'algorithme se termine effectivement puisque $sp_T(K_4)$ existe et est bornée par $3|T|$. En effet, on sait que $sp_T(G) \leq |T|(\chi(G)-1)$ (Tesman, 1989), donc que $sp_T(K_4) \leq 3|T|$.

Le fait que dans le T-graphe d'ordre $sp_T(K_4)$ il existe un sous-graphe isomorphe à K_4 tel que 0 et $sp_T(K_4)$ soient des sommet de ce sous-graphe implique que la valeur retournée est bien ce que l'on veut. En effet, à chaque itération i, on essaie de trouver un K_4 dans G_T^i puisqu'on veut que i, v_1 et v_2 soient à la fois adjacents au sommet 0 et qu'ils forment un triangle. Puisque la boucle s'effectue pour des i décroissants, la dernière valeur affectée à la variable retournée sera donc nécessairement la plus petite, c'est-à-dire $sp_T(K_4)$.

Il ne reste qu'à montrer que l'algorithme est bien polynomial. En effet, le nombre d'itérations effectuées est dans $\mathcal{O}(|T|)$. D'une part, la construction de G_T^i se fait dans $\mathcal{O}(|T|^2)$ et d'autre part, pour toute paire de sommets du voisinage de 0, on a $\mathcal{O}(|T|^2)$ telles paires, on vérifie si ces sommets et 0 forment un triangle, ce qui se fait en temps constant. Ainsi, au total on a $\mathcal{O}(|T|)$ itérations et pour chaque itération on effectue $\mathcal{O}(|T|^2)$ opérations. Donc au total l'agorithme s'effectue dans un temps appartenant à $\mathcal{O}(|T|^3)$, il s'agit donc bien d'un algorithme polynomial en $|T|$.

□

Algorithme pour T-colorer les roues paires

Notons d'abord que dans R_n il existe deux types de sommets, le sommet central et les autres sommets de la roue. On sait qu'un des sommets de R_n sera T-coloré avec la couleur 0.

Lemme 1.61. *Soit R_n une roue paire et soit c le sommet central de R_n, c'est-à dire le sommet de degré $n-1$. Alors il existe une T-coloration g de R_n de T-étendue optimale satisfaisant $g(c) \neq 0$.*

Preuve. En effet, soit f une T-coloration de R_n de T-étendue optimale. Notons $m = \max\{f(v) \mid v \in V(R_n)\}$. Supposons que le sommet central c soit T-coloré avec 0. Alors $g(v) = m - f(v)$ est une T-coloration de R_n dans laquelle le sommet c n'est pas T-coloré avec 0 et f et g ont évidemment la même T-étendue.

□

Suite au lemme précédent, il est suffisant, pour trouver une T-coloration de R_n, de considérer les deux cas possibles, c'est-à-dire, le cas où le sommet central est coloré avec la couleur $sp_T(R_n)$ et le cas où le sommet central est coloré avec une couleur comprise entre 1 et $sp_T(R_n) - 1$. Cette observation conduit à deux boucles distinctes dans l'algorithme que nous proposons. Comme pour l'algorithme 1.1 nous recherchons deux chemins de parités distinctes entre le sommet 0 et un autre sommet. Pour l'algorithme 1.1 ces deux chemins se trouvaient dans le T-graphe d'ordre i et nous notions L_i la somme des longueurs de ces chemins. Dans le cas présent, nous recherchons de tels chemins dans un sous-graphe du T-graphe d'ordre i, en fait il s'agit du sous-graphe induit par le voisinage d'un sommet correspondant au sommet central de la roue R_n. Pour cette raison, étant donné i l'ordre du T-graphe considéré, nous utiliserons la notation $\mathcal{L}_a^b$ pour désigner la somme des longueurs du plus court chemin pair et du plus court chemin impair allant de 0 à a dans le sous-graphe de G_T^i induit par $N(b)$, le voisinage du sommet b. Les conventions précédentes étant conservées.

Algorithme pour T-colorer R_n

Proposition 1.62. *Étant donné un T-ensemble et un entier pair n, l'algorithme 1.3 se termine en temps polynomial par rapport à $|T|$ en retournant $sp_T(R_n)$.*

Preuve. Tout d'abord, pour se convaincre que les bornes que nous utilisons pour l'agorithme sont satisfaisantes, il suffit d'une part de noter que toutes les roues paires

Algorithme 1.3 T-étendue de R_n

Antécédent: un T-ensemble et n un entier pair
Conséquent: la T-étendue de R_n

```
1: reponse = sp_T(K_4)
2: pour i = sp_T(K_4) − 1 à sp_T(K_3) faire
3:    Construire G_T^i
4:    si 0 ∈ N(i) alors
5:       Construire G_T^i[N(i)]
6:       pour tout B ∈ N(i) tel que 1 ≤ B < i faire
7:          si L_B^i ≤ n − 1 alors
8:             reponse = i
9:             Sortir de la boucle
10:         fin si
11:      fin pour
12:   fin si
13:   si reponse > i alors
14:      pour tout B ∈ N({0, i}) tel que 1 ≤ B < i faire
15:         Construire G_T^i[N(B)]
16:         si L_i^B ≤ n − 1 alors
17:            reponse = i
18:            Sortir de la boucle
19:         fin si
20:      fin pour
21:   fin si
22: fin pour
23: retourner (reponse)
```

contiennent un sous-graphe homomorphe à K_3 d'où $sp_T(R_n) \geq sp_T(K_3)$, et d'autre part que toutes les roues paires R_n, $n \geq 4$, sont homomorphes à K_4, d'où $sp_T(R_n) \leq sp_T(K_4)$, ceci est évident puisque tous les cycles impairs sont homomorphes à K_3. Donc les bornes que nous considérons sont bien valables et puisque nous avons déjà des algorithmes polynomiaux dans l'ordre de $|T|$ pour trouver $sp_T(K_3)$ et $sp_T(K_4)$, alors le nombre d'itérations de notre algorithme est borné.

Comme nous l'avons dit précédemment, notre algorithme se divise pricipalement en deux cas. Le cas où le sommet central est T-coloré avec la plus grande couleur, ce

qui est vérifié par la boucle aux lignes 4 à 9. Dans ces lignes nous supposons que i est le sommet central et nous recherchons l'image homomorphique d'un cycle impair d'ordre $n-1$ dans le voisinage du sommet i. Le second cas est le cas où le sommet central n'est pas T-coloré avec i, ce qui correspond aux lignes 13 à 18. Dans ces lignes, nous recherchons un sommet B tel que le voisinage contient l'image homomorphique d'un cycle impair d'ordre $n-1$ passant par les sommets 0 et i. Puisque toutes les valeurs pour $sp_T(R_n)$ sont ainsi vérifiées, l'algorithme retourne bien la T-étendue optimale de R_n, pour n un entier pair.

Comme $sp_T(K_4) - 1 \leq 3|T|$, on effectue un nombre d'itérations dans $\mathcal{O}(|T|)$. La construction de G_T^i s'effectue dans l'ordre de $\mathcal{O}(|T|^2)$ et après la construction de G_T^i on construit $G_T^i[N(i)]$ et $G_T^i[N(B)]$ dans un temps $\mathcal{O}(|T|)$. Les boucles correspondant aux lignes 6 et 14 de l'algorithme 1.3 sont dans $\mathcal{O}(|T|)$ et le calcul de $\mathcal{L}_B^i$ ou de $\mathcal{L}_i^B$ se fait dans $\mathcal{O}(|T|^2)$ puisqu'il suffit de considérer au plus i fois les voisinages d'un ensemble de sommets sur un graphe d'ordre i avec $i < 3|T|$. Ainsi, l'algorithme s'effectue donc dans un temps appartenant à $\mathcal{O}(|T|^4)$ et, par conséquent, cet algorithme est bien polynomial en $|T|$.

□

1.5.3 Les subdivisions de roues

Dans cette section nous nous intéressons aux subdivisions de roues. Une *subdivision* d'un graphe G est un graphe obtenu en remplaçant certaines arêtes de G par des chemins de longueur quelconque.

Nous avons vu dans la section précédente qu'une roue paire n'est pas 3-colorable et qu'une roue impaire est 3-colorable. Le théorème suivant caractérise la k-colorabilité des subdivisions de roues avec au moins une arête subdivisée.

Théorème 1.63. *Soit S_{R_n} une subdivision de R_n, $n \geq 4$, avec au moins une arête subdivisée. Alors, S_{R_n} est 3-colorable.*

Preuve. Soit c le sommet central de S_{R_n} et soit v un sommet de degré 2. Supposons S_{R_n} plongé dans le plan de façon que le sommet c ne soit pas sur la face extérieure.

Si v est un sommet de la face extérieure alors $\{c, v\}$ est un ensemble indépendant et $S_{R_n}[V - \{c, v\}]$ est un arbre. Par conséquent, S_{R_n} est 3-colorable.

Si v est un sommet sur un rayon de S_{R_n} alors il existe un sommet w de degré 3 sur la face extérieure tel que $\{c, w\}$ est un ensemble indépendant. Le graphe $S_{R_n}[V - \{c, w\}]$ est une forêt. Par conséquent, S_{R_n} est 3-colorable.

□

Corollaire 1.64. *Soit S_{R_n} une subdivision de R_n avec au moins une arête subdivisée. On a*

$$sp_T(S_{R_n}) \leq sp_T(K_3).$$

Corollaire 1.65. *Soit S_{R_n} une subdivision de R_n avec au moins une arête subdivisée. Si S_{R_n} contient un triangle alors on a*

$$sp_T(S_{R_n}) = sp_T(K_3).$$

Preuve. Par le théorème 1.63, S_{R_n} est 3-colorable. Il existe donc un homomorphisme de S_{R_n} dans K_3, et K_3 est un sous graphe de S_{R_n}. Le core de S_{R_n} est donc K_3. La proposition 1.53 termine la preuve.

□

Cas particulier des subdivisions de K_4

Nous considérons maintenant le cas de $R_4 \cong K_4$ qui est la roue d'ordre minimal. Les résultats suivants caractérisent les subdivisions de K_4 qui sont des cores.

Remarque 1.66. *Notons d'abord, qu'une subdivision de K_4 possède quatre sommets de degré 3 et tous les autres sommets sont de degré 2; nous noterons ces sommets w, x, y et z. Dans ce qui suit, nous supposerons que les subdivisions de K_4 sont plongées dans le plan de manière à ce que la face extérieure soit le plus petit cycle impair. Le sommet central sera toujours noté w et nous noterons les faces $F_{w,x,y}$, $F_{w,x,z}$, $F_{w,y,z}$ et $F_{x,y,z}$, selon les sommets de degré 3 appartenant à la face. Ainsi la face $F_{x,y,z}$ sera toujours la face extérieure. La Figure 1.6 illustre cette notation.*

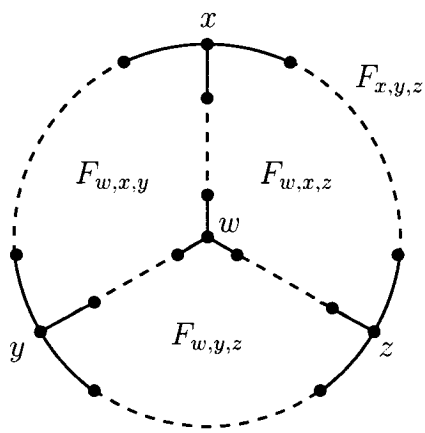

FIGURE 1.6 – *Convention de plongement d'une subdivision de K_4 dans le plan.*

Voici maintenant quelques résultats qui nous seront utiles pour poursuivre notre étude.

Définition 1.67. *On définit les θ-graphes comme les graphes formés par l'union de deux cycles avec une arête commune. Un θ-graphe généralisé est formé de deux sommets joints par trois chemins disjoints.*

Lemme 1.68. *Si G est un θ-graphe généralisé non biparti alors le core de G est le plus petit cycle impair contenu dans G.*

Preuve. La preuve de ce lemme est évidente.

□

Définition 1.69. *Notons R le multigraphe formé d'un triangle avec deux arêtes doubles. Nous dirons qu'un graphe est de la forme 1 s'il s'agit d'une subdivision de R qui est un graphe simple.*

Remarque 1.70. *G est de la forme 1 s'il est formé de trois sommets u,v et w tels qu'on ait deux chemins disjoints, P_2 et P_3, de u à v, deux chemins disjoints, P_1 et P_4 de u à w et un chemin P_5 de v à w. La Figure 1.7 illustre cette affirmation.*

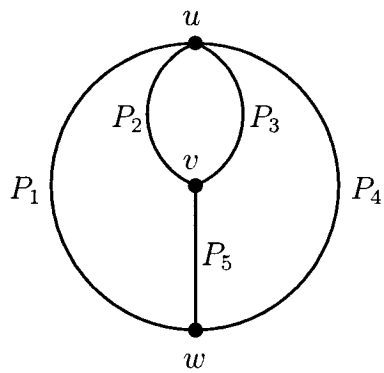

FIGURE 1.7 – *Graphe de la forme 1.*

Lemme 1.71. *Si G est de la forme 1 et non biparti alors le core de G est le plus petit cycle impair qu'il contient.*

Preuve. Pour prouver ce lemme nous déterminons un homomorphisme de G dans le plus petit cycle impair qu'il contient. Notons d'abord que si les chemins P_1 et P_4 ont des longueurs de même parité, (sans perte de généralité supposons que $|P_1| \leq |P_4|$), alors P_4 est homomorphe à P_1 et par conséquent G est homomorphe au graphe obtenu en enlevant toutes les arêtes et les sommets internes de P_4. Le graphe obtenu par cette opération est un θ-graphe généralisé. Le core de G est donc, par le lemme 1.68,

le plus petit cycle impair contenu dans G. Le résultat est le même si on suppose que P_2 et P_3 ont des longueurs de mêmes parités.

Supposons donc, sans perte de généralité, que $|P_1|$ et $|P_2|$ sont impairs et que $|P_3|$ et $|P_4|$ sont pairs. On note alors que les cas où le plus petit cycle impair est $P_1 \cup P_4$ ou $P_2 \cup P_3$ sont symétriques. Sans perte de généralité supposons donc que $P_1 \cup P_4$ est le plus petit cycle impair de G. Dans ce cas, on identifie les sommets de P_2 aux sommets de P_3, dans l'ordre d'apparition à partir du sommet v, créant ainsi un nouveau graphe G' avec des chemins P_2', P_3' et P_5' et un nouveau sommet v' commun à ces trois chemins. On effectue cette identification jusqu'à ce que $|P_2' \cup P_3'| = |P_1 \cup P_4|$ ou jusqu'à ce qu'on atteigne le sommet u. Si l'on atteint le sommet u avant que $|P_2' \cup P_3'| = |P_1 \cup P_4|$ alors G' consiste en un θ-graphe généralisé avec un cycle pendant au sommet u. Si le cycle est impair alors il est d'ordre au moins $|P_1 \cup P_4|$, et le lemme 1.68 nous assure de l'homomorphisme voulu.

Si au contraire on obtient que $|P_2' \cup P_3'| = |P_1 \cup P_4|$ avant d'atteindre le sommet u alors, en renotant P_2' le nouveau chemin de longueur impaire et P_3' le nouveau chemin de longueur paire, on obtient, si P_5' est de longueur paire, $|P_2' \cup P_5'| \geq |P_1|$ et $|P_3' \cup P_5'| \geq |P_4|$. On identifie alors deux sommets à distance deux de P_5' jusqu'à ce que $|P_2' \cup P_5'| = |P_1|$ ou que $|P_3' \cup P_5'| = |P_4|$. On peut alors identifier P_1 à $P_2' \cup P_5'$ ou bien P_4 à $P_3' \cup P_5'$. Le graphe obtenu est un θ-graphe et le lemme 1.68 termine la preuve. Si P_5' est de longueur impaire alors $|P_3' \cup P_5'| \geq |P_1|$ et $|P_2' \cup P_5'| \geq |P_4|$. On identifie alors deux sommets à distance deux de P_5' jusqu'à ce que $|P_3' \cup P_5'| = |P_1|$ ou que $|P_2' \cup P_5'| = |P_4|$. On peut alors identifier P_1 à $P_3' \cup P_5'$ ou bien P_4 à $P_2' \cup P_5'$. De nouveau, le graphe obtenu est un θ-graphe et le lemme 1.68 termine la preuve.

Il nous reste à vérifier le cas où le plus petit cycle impair est formé de trois chemins, c'est-à-dire $P_1 \cup P_2 \cup P_5$ ou $P_4 \cup P_2 \cup P_5$, si P_5 est de longueur impaire, et $P_1 \cup P_3 \cup P_5$ ou $P_4 \cup P_3 \cup P_5$, si P_5 est de longueur paire. Puisque le raisonnement est essentiellement le même dans tous les cas, nous ne traiterons que le cas où le plus

petit cycle impair est $P_1 \cup P_2 \cup P_5$. Dans ce cas P_5 est impair et on a $|P_3| \geq |P_1 \cup P_5|$ et $|P_4| \geq |P_2 \cup P_5|$. Puisque $|P_3| \geq |P_1 \cup P_5|$ alors P_3 est homomorphe à $P_1 \cup P_5$. De même, puisque $|P_4| \geq |P_2 \cup P_5|$ alors P_4 est homomorphe à $P_2 \cup P_5$. Ainsi, le graphe G est bien homomorphe au cycle $P_1 \cup P_2 \cup P_5$ tel que voulu.

Puisque dans tous les cas le graphe G est homomorphe à un cycle impair qui est un sous-graphe de lui-même alors le core d'un graphe de la forme 1 est bien un cycle impair.

□

Lemme 1.72. *Soit S_{K_4} une subdivision de K_4 qui n'est pas un core et qui n'est pas biparti. Alors le core de S_{K_4} est un cycle impair.*

Preuve. Notons H le core de S_{K_4}. Puisque S_{K_4} n'est pas un core, alors H est un sous-graphe de S_{K_4}. Or, si on enlève un sommet ou une arête à S_{K_4} alors le graphe obtenu est un θ-graphe généralisé, si on élimine les sommets pendants. Ainsi, par le lemme 1.68, le core de S_{K_4} est un cycle impair.

□

Puisque S_{K_4} est un graphe planaire ayant quatre faces, le nombre de faces impaires de ce graphe doit être pair. Si S_{K_4} ne contient aucune face impaire alors le graphe est biparti et son core est K_2. Les deux prochains résultats vérifient les cas où S_{K_4} possède deux faces impaires ou quatres faces impaires.

Dans ce qui suit, pour i et j des sommets de degré 3 dans une subdivision de K_4, nous noterons $\ell(i,j)$ la longueur du chemin allant de i à j et passant uniquement par des sommets de degré 2.

Théorème 1.73. *Soit S_{K_4} une subdivision de K_4 possédant deux faces paires et deux faces impaires, plongée dans le plan selon nos conventions. Par la remarque 1.66, $F_{x,y,z}$ est une face impaire, et disons que l'autre face impaire est $F_{w,x,z}$. Le core de S_{K_4} est un cycle impair si et seulement si une des deux conditions suivantes est vérifiée :*

a) $|F_{x,y,z}|$ *est la maille impaire de* S_{K_4},
$\ell(x,y) \leq \ell(w,x) + \ell(w,y)$ *et*
$\ell(y,z) \leq \ell(w,y) + \ell(w,z)$.

b) Aucune face n'a comme degré la maille impaire de S_{K_4}.

Preuve. $\Rightarrow$) Si le core de S_{K_4} est un cycle impair alors il s'agit bien sûr du plus petit cycle C qui est un sous-graphe de S_{K_4}. Si C est une face de S_{K_4} alors $C \cong F_{x,y,z}$ (selon notre convention) et disons que $|F_{x,y,z}| = 2k+1$ est la maille impaire de S_{K_4}. De manière équivalente on peut dire que le core de S_{K_4} est C_{2k+1}, les sommets de C_{2k+1} étant $1, 2, \ldots, 2k+1$. Considérons maintenant une C_{2k+1}-coloration de S_{K_4}, c'est-à-dire un homomorphisme de S_{K_4} dans C_{2k+1}. Supposons sans perte de généralité que la C_{2k+1}-coloration f affecte aux sommets x la couleur 1, y la couleur m et z la couleur n, avec $1 < m < n \leq 2k+1$. Puisque $F_{w,x,y}$ est pair alors $\ell(x,y)$ et $\ell(w,x) + \ell(w,y)$ sont de même parité. Pour partir de la couleur m et retourner à la couleur 1, sur un chemin de la même parité que $m-1$, avec des couleurs successives, il faut nécessairement passer par la suite $m-1, m-2, ..., 2$. D'où

$$\ell(x,y) \leq \ell(w,x) + \ell(w,y).$$

En utilisant le même raisonnement, on obtient également

$$\ell(y,z) \leq \ell(w,y) + \ell(w,z).$$

D'où la condition a).

Si C n'est pas une face de S_{K_4} alors $|F_{x,y,z}|$ n'est pas la maille impaire de S_{K_4} et selon la convention de la remarque 1.66 que nous observons, aucune face de S_{K_4} n'a pour degré la maille impaire de S_{K_4}. D'où la condition b).

$\Leftarrow$) Étant donné la condition a), considérons $P_{w,x} = [w, x_1, x_2, ..., x_p, x]$ et $P_{w,z} = [w, z_1, z_2, ..., z_q, z]$ les chemins allant de w à x et à z, respectivement, sans passer par des sommets de degré 3. Supposons sans perte de généralité que $q \geq p$. On identifie successivement les sommets x_i à z_i jusqu'à ce que la face formée par les sommets x, z et z_i soit d'ordre égale à $|F_{x,y,z}|$ ou jusqu'à ce que x soit identifié à z_i.

Si x est identifié à z_i alors le graphe obtenu est de la forme 1 et le lemme 1.71 nous indique qu'il existe une C_{2k+1}-coloration.

Dans l'autre cas, on obtient une subdivision de K_4 avec deux faces impaires de même ordre. Notons $P_{x,z_i,z}$ et $P_{x,y,z}$ les chemins allant de x à z en passant par z_i et y respectivement. Ces deux chemins sont de même longueur et peuvent donc être identifier sommet par sommet. Les sommets du chemin $P_{z_i,y}$, allant de z_i à y en ne passant par aucun sommet de degré 3, peuvent également être identifiés à des sommets de $P_{x,y,z}$ puisqu'on a

$$\ell(x,y) \leq \ell(w,x) + \ell(w,y) = \ell(z_i,x) + \ell(z_i,y), \text{ et}$$

$$\ell(y,z) \leq \ell(w,y) + \ell(w,z) = \ell(z_i,y) + \ell(z_i,z).$$

Il existe donc un homomorphisme de S_{K_4} dans $F_{x,y,z}$ et le core de S_{K_4} est bien un cycle impair.

Étant donné la condition b), le plus petit cycle impair C de S_{K_4} passe donc par les quatre sommets de degré 3, c'est-à-dire w, x, y et z. Renommons ces sommets a, b, c et d de manière à ce que l'on puisse considérer que C passe successivement par a, b, c et d. Il existe alors un unique chemin dans S_{K_4} allant du sommet a au sommet c sans passer ni par b, ni par d, notons-le $P_{a,c}$. Ce chemin est soit de même parité que le chemin allant de a à c en passant uniquement par b, noté $P_{a,b,c}$ ou soit de même parité que le chemin allant de a à c en passant uniquement par d, noté $P_{a,d,c}$. Supposons sans perte de généralité que $P_{a,c}$ soit de même parité que $P_{a,b,c}$

alors on a$|P_{a,c}| \geq |P_{a,b,c}|$, sinon la face $F_{a,c,d}$ est d'ordre inférieur à $|C|$ ce qui est une contradiction. On a donc un homomorphisme de $P_{a,c}$ dans $P_{a,b,c}$. De la même façon, on obtient un homomorphisme de $P_{b,d}$ dans $P_{b,c,d}$ ou un homomorphisme de $P_{b,d}$ dans $P_{b,a,d}$. On peut alors conclure qu'il existe un homomorphisme de S_{K_4} dans C ou de façon équivalente que C est le core de S_{K_4}.

□

Corollaire 1.74. *Soit S_{K_4} une subdivision de K_4 possédant deux faces paires et deux faces impaires. Le core de S_{K_4} est le cycle impair qui a pour ordre la maille impaire de S_{K_4}.*

Preuve. En effet, nous avons vu dans la démonstration du théorème 1.73 que peu importe le cycle impair C de S_{K_4}, que ce soit une face ou non, qui a pour ordre la maille impaire de S_{K_4}, on a toujours $S_{K_4} \to C$.

□

Nous traitons maintenant le cas des subdivisions de K_4 ayant quatre faces impaires. Notons d'abord qu'aucun cycle élémentaire, c'est-à-dire un cycle dont tous les sommets sont distincts, passant par les quatre sommets de degré 3 d'une subdivision de K_4 avec quatre faces impaires ne peut être d'ordre impair. Le cas de ce genre de cycle, qui devait être traité au théorème 1.73, n'a donc pas à être considéré ici. Autrement dit, si le core d'une subdivision de K_4 avec quatre faces impaires est un cycle impair, alors il s'agit nécessairement d'une face du graphe.

Théorème 1.75. *Soit S_{K_4} une subdivision de K_4 possédant quatre faces impaires, plongée dans le plan selon nos conventions. Le core de S_{K_4} est un cycle impair si et seulement si une des conditions suivantes est vérifiée :*

$$\deg(F_{x,y,z}) + \ell(x,y) \leq \ell(w,x) + \ell(w,y),$$

$$\deg(F_{x,y,z}) + \ell(y,z) \leq \ell(w,y) + \ell(w,z),$$

$$\deg(F_{x,y,z}) + \ell(x,z) \leq \ell(w,x) + \ell(w,z).$$

Preuve. $\Leftarrow$) Supposons sans perte de généralité que la première condition soit vraie, c'est-à-dire que $\deg(F_{x,y,z}) + \ell(x,y) \leq \ell(w,x) + \ell(w,y)$. Alors, il existe un sommet v appartenant à $P_{w,x}$ tel que $\ell(v,x) = \ell(x,y)$ ou il existe un sommet u appartenant à $P_{w,y}$ tel que $\ell(u,y) = \ell(x,y)$. Si v satisfait la propriété alors on peut identifier v et y et obtenir un nouveau graphe qui est de la forme 1 et tel que l'ordre minimal des cycles impairs est le même. Donc par le lemme 1.71 il existe une $C_{|P_{x,y,z}|}$-coloration de S_{K_4}. Le même résultat est obtenu si on choisit u plutôt que v.

Le même raisonnement s'applique aux deux autres conditions pour obtenir que le core de S_{K_4} est un cycle impair.

$\Rightarrow$) Disons que $|F_{x,y,z}| = 2p+1$. Soit f une C_{2p+1}-coloration de S_{K_4} telle que $f(x) = 1$, $f(y) = m$, $f(z) = n$, $n \geq m$, et $f(w) = k$. Si $k < m$ alors il existe un sommet v dans $P_{w,z}$ tel que $f(v) = 1$ ou $f(v) = m$, si $k > m$ alors il existe un sommet v dans $P_{w,x}$ tel que $f(v) = m$ ou $f(v) = n$ et si $k = m$ alors il existe un sommet v dans $P_{w,y}$ tel que $f(v) = 1$ ou $f(v) = n$.

Supposons sans perte de généralité que dans $P_{w,x}$ il existe un sommet coloré m ou n. Disons que la première couleur rencontrée en parcourant$P_{w,x}$ à partir de x est la couleur n pour un sommet v'. Alors, en identifiant v' à z, on obtient un graphe de la forme 1. On a deux cas possibles.

Si $\ell(v',x) \equiv \ell(x,z) \mod 2$, alors

$$\ell(v',x) \geq \ell(x,z), \text{ et}$$

$$\ell(v',w) + \ell(w,z) \geq \deg(F_{x,y,z}).$$

On a donc

$$\deg(F_{x,y,z}) + \ell(x,z) \leq \ell(w,x) + \ell(w,z).$$

Si $\ell(v',x) \not\equiv \ell(x,z) \mod 2$, alors

$$\ell(v',x) + \ell(x,z) \geq \deg(F_{x,y,z}), \text{ et}$$

il existe un sommet v'' appartenant au chemin $P_{x,v'}$ tel que $f(v'') = m$. Ceci contredit le fait que la première couleur rencontrée sur le chemin $P_{w,x}$ à partir de x est la couleur n. On doit donc avoir $\ell(v',x) \equiv \ell(x,z) \mod 2$, et la conclusion qui s'ensuit.

Par symétrie, on obtient le même résultat si on suppose au départ que la première couleur rencontrée est m plutôt que n. Dans ce cas, on obtient la condition

$$\deg(F_{x,y,z}) + \ell(x,y) \leq \ell(w,x) + \ell(w,y).$$

Avec le même raisonnement que ci-dessus, si on suppose que dans le chemin $P_{w,y}$ il existe un sommet coloré 1 ou n alors on obtient, respectivement, les conditions

$$\deg(F_{x,y,z}) + \ell(x,y) \leq \ell(w,x) + \ell(w,y), \text{ ou}$$

$$\deg(F_{x,y,z}) + \ell(y,z) \leq \ell(w,y) + \ell(w,z).$$

De même, si on suppose que dans le chemin $P_{w,z}$ il existe un sommet coloré 1 ou m alors on obtient, respectivement, les conditions

$$\deg(F_{x,y,z}) + \ell(x,z) \leq \ell(w,x) + \ell(w,z), \text{ ou}$$

$$\deg(F_{x,y,z}) + \ell(y,z) \leq \ell(w,y) + \ell(w,z).$$

□

Le corollaire suivant, issu des résultats précédents, caractérise entièrement les cores pour les subdivisions de K_4.

Corollaire 1.76. *Soit S_{K_4} une subdivision non biparti de K_4. Le core de ce graphe est S_{K_4} lui-même si, en respectant la convention de la remarque 1.66, on a*

$$\deg(F_{x,y,z}) + \ell(x,y) \geq \ell(w,x) + \ell(w,y),$$

$$\deg(F_{x,y,z}) + \ell(y,z) \geq \ell(w,y) + \ell(w,z), \text{ et}$$

$$\deg(F_{x,y,z}) + \ell(x,z) \geq \ell(w,x) + \ell(w,z).$$

Sinon, le core de S_{K_4} est le cycle impair ayant pour ordre la maille impaire de S_{K_4}.

Preuve. La preuve est directe en utilisant le lemme 1.72 et les deux théorèmes précédents.

□

Remarque 1.77. *Le corollaire précédent nous indique qu'il est possible de déterminer en temps polynomial une T-coloration de T-étendue optimale pour une subdivision de K_4 si le graphe lui-même n'est pas un core. En effet, il suffit alors de trouver la maille impaire du graphe et ensuite d'appliquer l'algorithme 1.1 pour la T-étendue des cycles impairs. Les homomorphismes utilisés dans les preuves des théorèmes 1.73 et 1.75 nous permettent ensuite de terminer la T-coloration.*

Pour conclure cette section sur la T-étendue des subdivisions de roues nous rappelons, sous forme d'un théorème, les bornes que nous avons obtenues sur la T-étendue pour les graphes appartenant à cette famille.

Théorème 1.78. *Soit S_{R_n} une subdivision non biparti de la roue R_n, avec $n \geq 3$, ayant au moins un sommet de degré 2. Si $2k+1$ est la maille impaire de S_{R_n} alors pour tout T-ensemble on a*

$$sp_T(C_{2k+1}) \leq sp_T(S_{R_n}) \leq sp_T(K_3).$$

Preuve. Puisque $2k+1$ est la maille impaire de S_{R_n} alors on a $C_{2k+1} \to S_{R_n}$, d'où la première inégalité. Le corollaire 1.64 nous donne l'autre inégalité.

□

Notons que la maille impaire d'une subdivision d'une roue est facile à obtenir puisqu'une subdivision de R_{n+1} possède exactement $n^2 - n + 1$ cycles distincts. Avec l'aide de l'algorithme 1.1 on peut alors obtenir très rapidement les bornes du théorème 1.78.

1.5.4 Les graphes 3-colorables

Pour investiguer le problème de la T-étendue des graphes 3-colorables, c'est-à-dire dont le nombre chromatique est 3, nous utilisons la notions de H-coloration et la notion de T-graphe, définie dans la section 1.3.5. En effet, par définition du T-graphe d'ordre n, noté G_T^n, l'ordre des sommets induit une T-coloration et tout graphe de T-étendue n est homomorphe à G_T^n. Il est donc possible, étant donné T, de tirer de l'information sur l'étendue des T-colorations en considérant les sous-graphes de G_T^n et les homomorphismes vers ces sous-graphes. Dans ce qui suit, nous présentons quelques résultats sur ce sujet, mais tout d'abord voici un lemme qui nous sera utile.

Lemme 1.79. *Soit G un graphe non biparti tel que $G - u$ et $G - v$ soient bipartis pour u et v deux sommets de G. Alors on peut déterminer la maille impaire de G en temps polynomial.*

Preuve. Puisque G possède un cycle impair et que tous les cycles impairs de G passent par les sommets u et v, alors aucun chemin pair entre u et v n'intersecte un chemin impair allant de u à v. Ainsi, un cycle ayant pour ordre la maille impaire de G est donc constitué des plus courts chemins pair et impair allant de u à v. Le procédé suivant nous permet de trouver la maille impaire de G. On trouve d'abord la distance entre u et v, disons d. Si d est pair, on enlève toutes les arêtes des chemins de longueur d et on réitère le processus tant qu'on n'obtient pas une distance impaire entre u et v. On obtient de cette manière la maille impaire de G. De la même façon, si au départ d est impair la même procédure s'applique, et on obtient également la maille impaire de G. Puisque trouver la distance entre deux sommets et un chemin associé se fait en temps polynomial, le procédé décrit s'effectue en temps polynomial.

□

Ce lemme sera utilisé dans l'algorithme qui suit. Cet algorithme reçoit en entrée un T-ensemble et retourne le plus petit entier k tel que G_T^k n'est pas biparti ainsi que la maille impaire de G_T^k.

Algorithme 1.4 Borne pour les graphes 3-colorables

Antécédent: un T-ensemble
Conséquent: le plus petit entier k tel que G_T^k n'est pas biparti et $2m+1$ la maille impaire de G_T^k

1: $i = 2$
2: Construire G_T^i
3: **tant que** G_T^i est biparti **faire**
4: $\quad i = i + 1$
5: $\quad$ Construire G_T^i
6: **fin tant que**
7: $\mathtt{k} = i$
8: Calculer `2m+1`, la maille impaire de $G_T^{\mathtt{k}}$
9: **retourner** `k` et `2m+1`

La valeur de k est bornée par $sp_T(K_3)$, l'algorithme se termine donc nécessairement après un nombre d'itérations dans $\mathcal{O}(|T|)$. Comme nous l'avons déjà dit, la

construction de G_T^i s'effectue en temps polynomial ($\mathcal{O}(|T|^2)$) et, par le lemme 1.79, le calcul de la maille impaire de G_T^k s'effectue en temps polynomial puisqu'on fait $\mathcal{O}(|T|^2)$ recherches du plus court chemin. Le calcul de la maille impaire de G_T^k est donc dans $\mathcal{O}(|T|^4)$ et par conséquent, l'algorithme 1.4 est un algorithme polynomial appartenant à $\mathcal{O}(|T|^5)$.

Observons que pour tout cycle impair d'ordre $2n+1$, $n \geq m$, on a $sp_T(C_{2n+1}) = k$. Ainsi, l'algorithme 1.4 permet donc de déterminer des bornes pour les graphes non bipartis en considérant seulement le T-ensemble qui a été fourni. Ceci est le sujet du résultat suivant.

Théorème 1.80. *Étant donné T, on considère le plus petit entier k tel que G_T^k n'est pas biparti retourné par l'algorithme 1.4 appliqué à l'ensemble T. Alors pour tout graphe 3-colorable non biparti G on a*

$$k \leq sp_T(G) \leq sp_T(K_3).$$

Preuve. En effet, G est 3-colorable implique que $G \to K_3$ et ainsi $sp_T(G) \leq sp_T(K_3)$. D'autre part, le T-graphe G_T^{k-1} est biparti implique qu'aucun cycle impair ne possède une T-étendue inférieure à k. De plus, puisque G est non biparti alors G contient un cycle, disons d'ordre $2p+1$. Ainsi $C_{2p+1} \to G$ et alors $k \leq sp_T(C_{2p+1}) \leq sp_T(G)$.

□

Puisqu'un graphe non biparti contient nécessairement un cycle impair, k est une borne inférieure pour ces graphes.

Corollaire 1.81. *Étant donné T, si k est le plus petit entier tel que G_T^k n'est pas biparti alors pour tout graphe G non biparti, on a $k \leq sp_T(G)$.*

Il est possible d'obtenir une condition nécessaire et suffisante pour qu'un graphe G ait pour T-étendue la borne k, c'est-à-dire le plus petit entier tel que G_T^k n'est pas biparti. Ceci est le sujet du prochain résultat.

Théorème 1.82. *Pour T donné, notons k le plus petit entier tel que G_T^k n'est pas biparti. Si $2m+1$ est la maille impaire de G_T^k alors pour tout graphe 3-colorable non biparti G on a*

$$sp_T(G) = k \Leftrightarrow G \to C_{2m+1}.$$

Preuve. Si $G \to C_{2m+1}$ alors $sp_T(G) \leq sp_T(C_{2m+1}) = k$. Par le théorème 1.80 on a que $sp_T(G) \geq sp_T(C_{2m+1}) = k$. Ainsi, on a bien $sp_T(G) = k$.

Supposons que $sp_T(G) = k$. Il faut montrer que $G \to C_{2m+1}$. Il suffit de montrer que $G_T^k \to C_{2m+1}$ puisque $G \to G_T^k$. En effet, rappelons que dans G_T^k aucun chemin pair allant du sommet 0 au sommet k n'intersecte de chemin impair allant de 0 à k. Considérons

$$I = \{v \in N(k) \mid v \text{ est sur un chemin impair de 0 à } k\}, \text{ et}$$

$$P = \{v \in N(k) \mid v \text{ est sur un chemin pair de 0 à } k\}.$$

Supposons que I et P sont des ensembles stables de sommets, sinon la maille impaire de G_T^k est 3 et le résultat est trivial.

Soit G' le graphe construit à partir de G_T^{k-1} dont les sommets dans I sont identifiés en un sommet i et les sommets dans P sont identifiés en un sommet p. Ces identifications correspondent à une suite d'homomorphismes élémentaires que nous notons g. Si nous notons P_{2m} le chemin d'ordre $2m$, alors il existe un homomorphisme surjectif f de G' dans P_{2m} avec les sommets i et p correspondant aux extrémités de P_{2m}. Le rajout d'un sommet x adjacent aux extrémités de P_{2m} nous donne un cycle C d'ordre $2m+1$. Les sommets de C peuvent alors être vus comme les éléments de $\{f \circ g(i) \mid i \in V(G_T^{k-1})\} \cup \{x\}$ et l'homomorphisme de G_T^k dans C_{2m+1} voulu est simplement donné par la fonction $h : V(G_T^k) \to V(C)$ définie par $h(i) = f \circ g(i)$ pour $0 \leq i \leq k-1$ et $h(k) = x$. Nous avons l'homomorphisme recherché, ce qui termine la preuve.

□

Remarque 1.83. *Les résultats précédents nous montre à quel point la notion de T-graphe peut être utile pour estimer la valeur de la T-étendue d'un graphe. Il est bien connu que le problème de coloration d'un graphe est un problème compliqué, toutefois puisque la construction d'un T-graphe ne dépend que du T-ensemble que l'on a, la complexité de déterminer le nombre chromatique d'un T-graphe varie selon T. Pour certains T-ensembles particuliers, il peut donc s'avérer avantageux de considérer une généralisation aux graphes n-colorables des résultats présentés ci-dessus. De manière générale, lors de la construction du T-graphe, on trouve le plus petit k tel que G_T^k ne soit pas $(n-1)$-colorable, on obtient alors la borne inférieure k pour tous les graphes n-colorables, $n \geq 3$.*

Pour donner un exemple de ce que l'on vient de dire, il suffit de considérer les T-ensembles de type r-initial ou k-multiples de s, définis à la section 1.3.3, pour lesquels nous avons

$$sp_T(G) = sp_T(K_{\chi(G)}).$$

En résumé, nous avons vu dans cette section qu'étant donné certaines structures de graphes, il est possible de déterminer en temps polynomial des T-colorations d'étendue optimale pour ces graphes. Nous avons, en particulier, donné des algorithmes pour les cycles impairs et les roues. Nous avons également montré que sous certaines conditions le core d'une subdivision de K_4 est un cycle impair, donc de T-étendue déterminable en temps polynomial. Puis nous avons donné des bornes pour les subdivisions de roues. Dans un cadre plus général, nous avons fourni un algorithme polynomial qui nous donne, quel que soit le T-ensemble choisi, des bornes sur la T-étendue des graphes 3-colorables.

CHAPITRE 2

RÈGLES DE GOLOMB

2.1 Généralités

2.1.1 Définition du problème

Définition 2.1. *Une règle de Golomb d'ordre J est un ensemble de $J+1$ entiers naturels,*

$$\Delta = \{m_0, m_1, \ldots, m_J\},$$

tel que toutes les différences

$$|m_{j'} - m_j|,$$

pour $0 \leq j < j' \leq J$, sont distinctes.

Les éléments d'une règle de Golomb sont appelés les *marques* de la règle. Étant donné une règle de Golomb Δ, pour référer à la j-ième marque de cette règle nous utiliserons la notation $m_j(\Delta)$. Lorsqu'il n'y a pas de confusion possible pour la règle en question, nous utiliserons simplement la notation m_j pour désigner la j-ième marque de la règle.

Remarque 2.2. *Dans une règle de Golomb, nous supposerons que les marques sont toujours en ordre croissant selon l'indice. Autrement dit, nous supposerons que*

$$j' > j \Rightarrow m_{j'} > m_j.$$

Selon cette convention, l'élément maximal d'une règle de Golomb, appelé longueur *de la règle, est donc toujours la marque m_J et il n'est pas nécessaire de considérer les*

valeurs absolues pour les différences entre les marques puisque toutes les différences seront alors positives.

Soit $\Delta = \{m_0, m_1, \ldots, m_J\}$ *une règle de Golomb avec* $m_0 > 0$. *Alors* $\Delta' = \{m_0 - m_0, m_1 - m_0, \ldots, m_J - m_0\}$ *est aussi une règle de Golomb. Puisque pour toute règle, il y a une règle équivalente avec* $m_0 = 0$, *nous supposerons toujours que la marque* m_0 *est égale à 0.*

Étant donné l'entier J, le minimum de $m_J(\Delta)$ pour toutes les règles de Golomb Δ d'ordre J est noté $M(J)$. Autrement dit, on pose

$$M(J) = \min\{m_J(\Delta) \mid \Delta \text{ est une règle de Golomb d'ordre } J\}.$$

Une règle de Golomb Δ qui satisfait $m_J(\Delta) = M(J)$ est dite *optimale.* Lorsque Δ satisfait $m_J(\Delta) = M(J) = \frac{J(J+1)}{2}$, c'est-à-dire que l'élément maximal de la règle de Golomb est égal au nombre de différences générées, nous dirons que Δ est une règle de Golomb *parfaite.*

Exemple 2.3. *L'ensemble* $\{0, 1, 4, 9, 11\}$ *est une règle de Golomb d'ordre 4 puisque les différences générées, illustrées dans le triangle des différences ci-dessous, sont toutes distinctes.*

0		1		4		9		11
	1		3		5		2	
		4		8		7		
			9		10			
				11				

Cette règle est optimale puisqu'il n'existe pas de règle de Golomb d'ordre 4 avec $m_4 < 11$. *Pour* $J = 4$, *il n'existe pas de règle de Golomb parfaite puisqu'il y a 10 différences générées et que* $M(4) = 11$.

La règle $\{0, 1, 4, 6\}$ *est un exemple de règle parfaite puisque, pour une règle d'ordre 3, il y a 6 différences générées et que* $M(3) = 6$. *En fait, Golomb (1972) a démontré que des règles parfaites existent seulement pour* $J \leq 3$.

Le problème qui consiste à déterminer une règle de Golomb optimale est appelé *problème de la règle de Golomb.*

2.1.2 Équivalence pour les règles de Golomb

Bien que nous ayons adopté la convention d'avoir toujours 0 pour valeur de la marque m_0 dans le problème de la règle de Golomb, il est important de faire les observations suivantes sur les règles de Golomb équivalentes. Étant donné une règle de Golomb $\Delta = \{m_0, m_1, \ldots, m_J\}$, on vérifie facilement pour $m' \in \mathbb{N}$ que

$$\Delta' = \{m_0 + m', m_1 + m', \ldots, m_J + m'\}$$

est aussi une règle de Golomb. De même, pour $m' \geq m_J$, on peut vérifier que

$$\Delta' = \{m' - m_J, m' - m_{J-1}, \ldots, m' - m_0\}$$

est aussi une règle de Golomb. Ces deux observations, bien qu'évidentes, seront utiles pour la construction de règles de Golomb par les méthodes dites algébriques à la section 2.3.

Soit $\Delta = \{m_0, m_1, \ldots, m_J\}$ une règle de Golomb. Alors la règle

$$\Delta' = \{m'_0 = m_J - m_J, m'_1 = m_J - m_{J-1}, \ldots, m'_J = m_J - m_0\}$$

est une règle de Golomb satisfaisant $m'_0 = 0$ telle que Δ' est le "miroir" de Δ. Dans un tel cas, nous dirons que les règles Δ et Δ' sont des *règles symétriques.* L'exemple suivant illustre bien la notion de symétrie entre deux règles de Golomb.

Exemple 2.4. *Pour illustrer la symétrie dans les règles de Golomb, reprenons la règle* $\{0, 1, 4, 9, 11\}$ *de l'exemple 2.3. Selon ce que nous venons de dire, la règle symétrique est alors* $\{11 - 11 = 0, 11 - 9 = 2, 11 - 4 = 7, 11 - 1 = 10, 11 - 0 = 11\}$. *En représentant ces deux règles par leur triangle des différences on voit bien la symétrie apparaître entre les différences de chaque règle.*

0	1	4	9	11	0	2	7	10	11
1	3	5	2		2	5	3	1	
4	8	7			7	8	4		
9	10				10	9			
11					11				

2.1.3 Applications des règles de Golomb

Les règles de Golomb sont des objets mathématiques qui ont été largement étudiés et on retrouve de nombreux travaux de recherche à leur sujet dans la littérature. Leurs applications sont nombreuses même s'il n'existe pas, à ce jour, d'algorithme très efficace permettant de déterminer une règle optimale pour un ordre voulu. Par conséquent, le problème demeure toujours un sujet d'actualité. Parmi les domaines d'application des règles de Golomb, on retrouve la cristallographie, la radio-astronomie, la radio-communication, la théorie du codage, etc. (Bloom et Golomb, 1978).

Application en cristallographie

Les résultats obtenus sur les règles de Golomb nous disent que, à l'exception d'un seul cas, deux règles de Golomb non symétriques de même ordre génèrent des ensembles de différences qui sont distincts (Bloom et Golomb, 1977). Ce résutat est utilisé pour l'analyse par rayons X de la structure des cristaux de la manière suivante. Tout d'abord, la position des atomes dans la structure d'un cristal est déterminée par des mesures obtenues à partir d'un patron de diffraction aux rayons X du cristal. Les mesures obtenues fournissent ensuite un ensemble de distances entre les atomes pour la structure cristallographique, ce qui permet généralement de distinguer deux cristaux. Toutefois, il peut arriver qu'il y ait ambiguïté entre deux structures cristallographiques si l'ensemble des distances entre les atomes est le même

pour les deux cristaux. Dans ce cas, à l'aide des règles de Golomb et en utilisant le fait mentionné ci-dessus, il est possible d'éviter qu'il y ait des ambiguïtés.

La seule paire de règles de Golomb non symétriques connue qui ne satisfait pas la condition d'avoir des ensembles de différences distincts est la paire de règles

$$\{0, 1, 8, 11, 13, 17\} \text{ et}$$

$$\{0, 1, 4, 10, 12, 17\},$$

pour lesquelles on peut vérifier que les différences générées sont les mêmes.

Applications en radio-astronomie

En radio-astronomie les règles de Golomb sont utilisées pour établir l'emplacement des antennes radar (Dewdney, 1985). En effet, comme nous le verrons, la manière optimale de disposer les antennes radar consiste à les placer sur une ligne droite, à des distances de plusieurs kilomètres, aux endroits correspondant aux marques d'une règle de Golomb. La raison pour laquelle cette disposition est intéressante est que pour localiser la source d'une onde radio, il est essentiel de déterminer l'angle entre la ligne des antennes et la direction de l'onde radio arrivant de la source. Pour ce faire les antennes sont alors ajustées pour recevoir à une même longueur d'onde et les temps précis auxquels chaque onde arrive aux antennes sont mesurés et comparés pour chaque paire d'antennes. La direction du signal peut alors être déterminée en analysant la différence de phase entre les paires d'antennes. La précision sur la différence de phase totale est optimale lorsqu'il n'y a pas deux paires d'antennes situées à la même distance, puisque des distances identiques correspondent à des différences de phase identiques. La disposition idéale consiste donc à situer les antennes selon les marques d'une règle de Golomb.

Une autre façon de localiser une source radio est d'utiliser seulement deux radars. Pour ce faire, il faut alors ajuster les antennes pour recevoir sur plusieurs longueurs

d'onde différentes. Encore une fois, la précision pour la localisation est optimale si les différences entre les paires de longueurs d'onde utilisées sont distinctes, c'est-à-dire si on utilise une règle de Golomb.

Application en radio-communication

La première application des règles de Golomb appartient au domaine de la radio-communication. Cette application, qui est due à Babcock (1953), concerne le problème d'affectation des fréquences radio. Ce problème consiste à affecter des fréquences aux différents émetteurs d'un réseau de façon à éviter les interférences. Les fréquences peuvent être associées à des nombres, qui peuvent être vus comme des entiers appartenant à un intervalle réel. Comme le nombre de fréquences disponibles est généralement restreint, on cherche à affecter des fréquences appartenant au plus petit intervalle possible.

L'apport des règles de Golomb consiste à éviter un certain type d'interférences appelé intermodulation. Ce phénomène survient lorsque plusieurs fréquences entrent en conflit et forment une nouvelle fréquence indésirable. On appelle intermodulation d'ordre trois les conflits de la forme

$$a_q + a_r - a_s = a_t \ ,$$

où a_q, a_r, a_s et a_t sont des fréquences disponibles dans l'intervalle alloué. Il est facile de voir que si les fréquences affectées aux émetteurs du réseau correspondent aux marques d'une règle de Golomb, alors l'intermodulation d'ordre trois est complètement enrayée.

Application en théorie du codage

La principale application des règles de Golomb appartient au domaine de la théorie du codage. Plusieurs types de codes correcteurs d'erreurs utilisent en effet les

règles de Golomb. L'idée des codes correcteurs d'erreurs est de générer un surplus d'information sur un message à envoyer, c'est-à-dire un mot d'un code sur l'alphabet $\{0, 1\}$, de façon à pouvoir décoder et valider le message reçu. Ce surplus d'information doit être généré de manière efficace pour minimiser la quantité d'information à transmettre. Étant donné un message binaire, en utilisant des registres aux endroits correspondants aux marques d'une règle de Golomb, il est possible lors du décodage d'obtenir une information non corrélée pour les bits du message envoyé. Ce type de code correspond aux codes convolutionnels auto-orthogonaux introduits par Massey (1963). Robinson et Bernstein (1967) ont obtenu ces codes à partir d'une généralisation des règles de Golomb appelée DTS, sujet qui sera traité en détail dans le chapitre suivant.

Autres applications

D'autres applications des règles de Golomb existent. Par exemple, il arrive souvent qu'une tâche informatique soit répartie sur plusieurs ordinateurs. Lorsque tous les ordinateurs fonctionnent, la tâche est distribuée de façon quasi-uniforme. Toutefois, lorsque que des bris surviennent sur les ordinateurs du réseau, il faut redistribuer les parties de tâches attribuées aux ordinateurs défaillants. Klonowska, Lundberg et Lennerstad (2003) proposent pour résoudre ce problème une méthode de recouvrement qui correspond à déterminer des règles de Golomb. Un autre exemple d'application appartient au domaine des communications PPM (pulse position modulation). Dans ce domaine, un problème consiste à trouver une séquence avec certaines propriétés d'autocorrélation, appelée séquence d'acquisition. Dans un article de Gagliardi, Robbins et Taylor (1987), les auteurs montrent comment de telles séquences, pour des cas particuliers, peuvent être obtenues à l'aide des règles de Golomb.

2.1.4 Bornes sur les règles de Golomb

Les règles de Golomb dont la longueur optimale est connue et prouvée sont les règles d'ordre $J \leq 23$. Pour un ordre donné, il existe plusieurs règles de longueur optimale, un exemple de règle optimale est donné dans le Tableau 2.1, pour chaque ordre J inférieur ou égal à 23.

En ce qui concerne les bornes supérieures, elles sont obtenues par construction, tout particulièrement par les méthodes dites algébriques, qui seront l'objet de la section 2.3. Les longueurs des meilleures règles de Golomb connues à ce jour, pour les règles d'ordre supérieur à 23, sont disponibles sur la page web de Shearer (n.d.).

En ce qui concernent les bornes inférieures, le lecteur peut se référer aux articles de Chen et Kløve (1991), de Hansen, Jaumard et Meyer (1999), ou encore de Kløve (1988; 1989; 1990). Encore une fois, les meilleures bornes inférieures connues à ce jour sont disponibles sur la page web de Shearer (n.d.).

La proposition suivante, due à Chen (1983), nous donne une formule algébrique pour obtenir analytiquement la meilleure borne inférieure connue sur les règles de Golomb.

Proposition 2.5. *Soit $J-1$ l'ordre de la règle de Golomb voulue. Si aucune marque n'est fixée, la formule suivante nous donne une borne inférieure S_0 pour la valeur de la marque $J-1$.*

$$S_0 = \left\lceil \max_{1 \leq k \leq \frac{J}{2}} \left\{ \frac{k}{k+1} J^2 - \frac{k^2+k-1}{k+1} J + \frac{1}{12}(k-1)(7k+10) \right\} \right\rceil .$$

2.1.5 Différentes approches

Pour résoudre le problème de la règle de Golomb, différentes approches ont été utilisées. Lorentzen et Nilsen (1991) ont, les premiers, donné un modèle de program-

TABLEAU 2.1 – Règles de Golomb optimales.

J	règle optimale d'ordre J
1	0,1
2	0,1,3
3	0,1,4,6
4	0,1,4,9,11
5	0,1,4,10,12,17
6	0,1,4,10,18,23,25
7	0,1,4,9,15,22,32,34
8	0,3,9,17,19,32,39,43,44
9	0,1,6,10,23,26,34,41,53,55
10	0,1,4,13,28,33,47,54,64,70,72
11	0,2,6,24,29,40,43,55,68,75,76,85
12	0,7,8,17,21,36,47,63,69,81,101,104,106
13	0,5,28,38,41,49,50,68,75,92,107,121,123,127
14	0,6,7,15,28,40,51,75,89,92,94,121,131,147,151
15	0,1,4,11,26,32,56,68,76,115,117,134,150,163,168,177
16	0,5,7,17,52,56,67,80,81,100,122,138,159,165,168,191,199
17	0,2,10,22,53,56,82,83,89,98,130,148,153,167,188,192,205,216
18	0,4,13,15,42,56,59,77,93,116,126,138,146,174,214,221,240,245,246
19	0,24,30,43,55,71,75,89,104,125,127,162,167,189,206,215,272,275,282,283
20	0,4,23,37,40,48,68,78,138,147,154,189,204,238,250,251,256,277,309,331,333
21	0,1,9,14,43,70,106,122,124,128,159,179,204, 223,253,263,270,291,330,341,353,356
22	0,6,22,24,43,56,95,126,137,146,172,173,201, 213,258,273,281,306,311,355,365,369,372
23	0,9,33,37,38,97,122,129,140,142,152,191,205, 208,252,278,286,326,332,353,368,384,403,425

mation linéaire en nombres entiers pour résoudre ce problème. Leur modèle sert en fait à résoudre le problème du DTS, une généralisation du problème de la règle de Golomb. Cette approche sera décrite plus en détail et dans le contexte général des DTS au chapitre suivant.

Il existe aussi des méthodes dites exactes dans lesquelles on énumère implicitement les solutions par différentes techniques de branchement. La méthode consiste à fixer

successivement des marques de la règle tant que c'est possible, puis à revenir à la marque précédente lorsqu'il n'est plus possible de fixer de nouvelles marques. La principale méthode de ce type est l'algorithme GARSP qui est décrit brièvement à la section 2.2.

Une autre approche consiste à utiliser certaines propriétés d'une structure algébrique pour déterminer des règles de Golomb. Ces méthodes qui sont appelées méthodes algébriques donnent présentement les meilleures valeurs connues pour les règles de Golomb dont l'optimalité n'est pas encore confirmée. Cette approche est décrite en détail à la section 2.3.

Une autre façon de voir les règles de Golomb d'ordre J est de considérer un étiquetage des sommets du graphe complet K_{J+1} avec des entiers positifs distincts. Si on affecte à chaque arête la valeur absolue de la différence des étiquettes de ses extrémités, on veut alors que les valeurs affectées aux arêtes soient toutes distinctes. Cette façon de voir les règles de Golomb nous permet donc de constater qu'il s'agit en fait d'une généralisation de la notion de graphe gracieux. En effet, pour qu'un graphe G, non nécessairement complet, soit dit gracieux, il doit exister un étiquetage tel que ci-dessus pour lequel l'ensemble des valeurs affectées aux arêtes soit $\{1, 2, ..., |E(G)|\}$. Les règles de Golomb qui correspondent à des étiquetages gracieux sont donc les règles d'ordre inférieur à 4, puisque, comme nous l'avons déjà dit, les seules règles de Golomb parfaites sont des règles d'ordre au plus 3. Le problème de la règle de Golomb d'ordre J peut donc, de manière informelle, être vu comme le problème de trouver un étiquetage le plus gracieux possible du graphe K_{J+1}. La Figure 2.1 illustre un étiquetage du graphe K_5 avec les éléments de la règle de Golomb $\{0, 1, 4, 9, 11\}$ de l'exemple 2.3.

Il existe plusieurs articles où le problème de la règle de Golomb est considéré comme un problème d'étiquetage des sommets d'un graphe. Le lecteur désirant avoir plus de détails sur les relations entre les règles de Golomb et les problèmes d'étiquetage de graphes peut consulter les articles de Golomb (1972) et de Bloom et Golomb

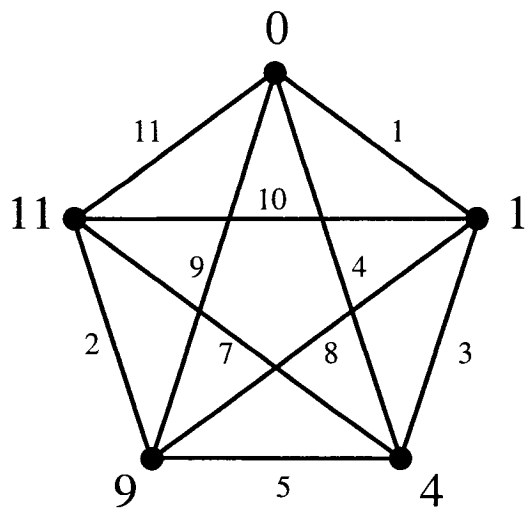

FIGURE 2.1 – *Étiquetage correspondant à une règle de Golomb*

(1978). Un autre ouvrage intéressant sur ce sujet est un article de Gibbs et Slater (1991), où la notion d'étiquetage des graphes correspondant à une règle de Golomb est généralisée en étiquetage par des vecteurs d'entiers.

2.2 Méthodes exactes

Les méthodes de résolution exacte du problème de la règle de Golomb sont essentiellement des méthodes d'énumération implicite avec bornes inférieures et supérieures. L'algorithme GARSP est un algorithme de ce type avec une stratégie d'exploration en profondeur d'abord. Il est en fait une amélioration de l'algorithme SHIFT introduit par Dollas, Rankin et McCracken (1998). Une brève description de l'algorithme GARSP est présentée dans cette section uniquement pour donner un aperçu de ce genre de méthode.

L'originalité de l'algorithme GARSP par rapport aux algorithmes habituels d'énumération implicite réside dans l'utilisation de structures d'accès et de mise à jour rapide, c'est-à-dire de vecteurs de bits (ou bitmaps). Les vecteurs de bits nécessaires

pour le fonctionnement de GARSP sont essntiellement les suivants :

LENGTH (contenant les positions des marques de la règle en cours de construction),

LIST (contenant les différences créées par la nouvelle marque ajoutée),

DIST (contenant toutes les différences dans la règle en cours de construction),

COMP (contenant les différences interdites pour les prochaines marques à fixer) et

FIRST (un vecteur permettant de déterminer la plus petite marque qu'il est possible d'utiliser pour obtenir une règle de Golomb d'ordre supérieur).

À chaque itération de GARSP on cherche à fixer une nouvelle marque pour la règle. On vérifie alors que la marque permette que la règle en construction puisse satisfaire les bornes inférieure et supérieure qui sont disponibles à ce niveau. Si une telle marque est obtenue alors les vecteurs décrits ci-dessus sont mis à jour, on ajuste la borne inférieure disponible et l'algorithme se poursuit ; sinon, on effectue un retour arrière, la marque fixée précédemment est modifiée, la borne inférieure est réajustée et les vecteurs sont mis à jour. Lorsque la dernière marque est fixée, on ajuste la borne supérieure si on a obtenu une meilleure règle, on enlève la dernière marque fixée et l'algorithme se poursuit ainsi jusqu'à ce qu'on retourne à la première marque et que l'on ait épuisé toutes les valeurs possibles pour cette marque.

Des variantes et des améliorations ont été apportées à GARSP (Hoa, 1999), mais l'idée centrale des méthodes exactes proposées dans la littérature reste toujours la même. La complexité du problème et l'incapacité d'obtenir des bornes inférieures de bonne qualité, c'est-à-dire l'incapacité de réduire l'énumération, font en sorte que ces méthodes ne sont efficaces, en temps de calcul, que pour des règles d'ordre limité.

2.3 Méthodes algébriques

2.3.1 Généralités sur les corps finis

Cette partie est consacrée aux différents résultats et définitions qui seront nécessaires pour présenter les méthodes algébriques de résolution du problème de la règle de Golomb. Nous rappelons tout d'abord les structures de groupe, d'anneau et de corps. Les résultats présentés dans ce texte, sous forme de rappels, sont restreints aux concepts essentiels, plus particulièrement pour ce qui se rapporte aux polynômes et aux extensions de corps. Le lecteur intéressé peut consulter le livre de Lidl et Niederreiter (1994) dans lequel on retrouve, de façon plus approfondie, les notions abordées dans cette section et les preuves des résultats énoncés.

Structures algébriques

Définition 2.6. *Un* groupe *est un ensemble G muni d'une opération binaire, notée $*$, tel que G est fermé sous cette opération (c'est-à-dire que pour tous a et b appartenant à G, $a * b$ appartient aussi à G) et les trois propriétés suivantes sont vérifiées :*

1. *$*$ est associative, c'est-à-dire que pour tous $a, b, c \in G$,*

$$a * (b * c) = (a * b) * c.$$

2. *Il existe dans G un élément identité, noté e, tel que pour tout $a \in G$,*

$$a * e = e * a = a.$$

3. *Pour tout $a \in G$, il existe un élément inverse $a^{-1} \in G$ tel que*

$$a * a^{-1} = a^{-1} * a = e.$$

De plus, si le groupe satisfait

4. *Pour tout* $a, b \in G$,

$$a * b = b * a,$$

alors le groupe est dit abélien (ou commutatif).

Pour les groupes, il existe deux types de notation : la notation multiplicative, lorsque l'opération du groupe est considérée comme la multiplication usuelle, et la notation additive, lorsque l'opération du groupe est considérée comme l'addition usuelle. Le groupe est alors dit *multiplicatif* ou *additif*, suivant le cas. En notation multiplicative, s'il n'y a pas de confusion possible pour les opérations de groupes, la multiplication de deux éléments est simplement notée par la concaténation des deux éléments, autrement dit, le produit $a * b$, des éléments a et b du groupe peut simplement être noté ab s'il n'y a pas de confusion possible sur l'opération en question.

Soit G un groupe multiplicatif et soit g un élément de G. Dans ce qui suit, lorsque l'élément g sera multiplié $n-1$ fois par lui-même, nous noterons g^n le résultat, en spécifiant que n appartient à $\mathbb{Z}$, n négatif voulant dire qu'il s'agit de l'opération inverse de la multiplication, c'est-à-dire que $g^{-n} = (g^n)^{-1}$.

Un groupe multiplicatif G est dit *cyclique* s'il existe un élément $a \in G$ tel que pour tout $b \in G$ il existe un entier j satisfaisant $b = a^j$. Dans ce cas, on dit que a est un *générateur* du groupe G et on écrit $G = \langle a \rangle$. De plus, lorsque $\langle a \rangle$ est un groupe fini, on appelle *ordre* de l'élément a l'ordre du groupe, c'est-à-dire le nombre d'éléments qui le composent.

Soit $\phi : G \to H$ une application du groupe G dans le groupe H. Si $*$ et $\cdot$ sont respectivement les opérations de G et de H, alors on dit que ϕ *préserve l'opération de* G si pour tout $a, b \in G$ on a

$$\phi(a * b) = \phi(a) \cdot \phi(b).$$

Définition 2.7. *Une application $\phi : G \to H$ du groupe G dans le groupe H est appelée un* homomorphisme de G dans H *si ϕ préserve l'opération de G. Un homomorphisme de G dans G est appelé un* endomorphisme. *Lorsque $\phi : G \to H$ est bijective on dit que ϕ est un* isomorphisme. *Un isomorphisme de G dans G est appelé un* automorphisme.

Définition 2.8. *Un* anneau $(R, +, \cdot)$ *est un ensemble R, muni des opérations binaires $+$ (addition) et $\cdot$ (multiplication), tel que R est fermé sous ces opérations et les conditions suivantes sont vérifiées :*

1. *R est un groupe abélien pour l'opération $+$,*
2. *l'opération $\cdot$ est associative, et*
3. *$\forall\, a, b, c \in R$, on a la propriété de distributivité*

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ et } (b + c) \cdot a = b \cdot a + c \cdot a.$$

Par convention, l'identité pour l'addition sera toujours notée 0.

Si $(R \setminus \{0\}, \cdot\,)$ forme un groupe abélien, on dit que $(R, +, \cdot\,)$ est un corps. *Dans le cas où R est un corps, il existe un élément identité pour le groupe multiplicatif. Dans le reste de ce texte, l'élément identité du groupe multiplicatif d'un corps sera toujours noté* 1.

La définition 2.7 pour les homomorphismes de groupes s'étend directement à une définition pour les anneaux ou pour les corps. C'est le sujet de la définition suivante.

Définition 2.9. *Une application $\phi : R \to S$ d'un anneau R dans un anneau S est appelée un* homomorphisme *si les opérations $+$ et $\cdot$ de R sont préservées et ϕ induit un homomorphisme du groupe additif de R sur le groupe additif de S. Dans le cas où R et S sont des corps, ϕ doit en plus induire un homomorphisme du groupe multiplicatif de $R \setminus \{0\}$ sur le groupe multiplicatif de $S \setminus \{0\}$.*

Les prochains résultats que nous présentons concernent les sous-anneaux et plus particulièrement les idéaux. Ces notions sont abordées dans le seul but de présenter l'anneau des classes résiduelles. Cet anneau sera ensuite utilisé sur l'anneau des polynômes pour obtenir les différents corps finis. Nous verrons en effet que tous les corps finis peuvent être obtenus à partir de ces structures particulières.

Définition 2.10. *Un sous-ensemble S d'un anneau R est un* sous-anneau de R *s'il est fermé pour l'addition et la multiplication et qu'il forme un anneau pour ces opérations.*

Définition 2.11. *Un sous-anneau J de R est un* idéal de R *si pour tout $a \in J$ et $r \in R$, les éléments $r \cdot a$ et $a \cdot r$ appartiennent à J.*

Remarque 2.12. *Soit R un anneau quelconque et soit r un élément de R. Dans ce qui suit, lorsque l'élément r sera additionné $n-1$ fois à lui-même, nous noterons nr le résultat, en spécifiant que n appartient à $\mathbb{Z}$, n négatif voulant dire qu'il s'agit de l'opération inverse de l'addition, c'est-à-dire que $-nr = n(-r)$.*

Soit a un élément de R. Nous noterons (a) l'ensemble $\{r \cdot a + na \mid r \in R, n \in \mathbb{Z}\}$. Si R contient une identité pour la multiplication alors $(a) = \{r \cdot a \mid r \in R\}$.

Définition 2.13. *Soit R un anneau commutatif. Un idéal J de R est dit* principal *s'il existe un $a \in R$ tel que $J = (a)$. On dit alors que J est l'anneau principal engendré par a.*

Étant donné un idéal J d'un anneau R, on peut définir une partition des éléments de R en classes résiduelles modulo J. La classe résiduelle d'un élément $a \in R$ est notée $[a] = a + J$ puisqu'elle est constituée des éléments de R de la forme $a + c$ pour un $c \in J$.

Deux éléments $a, b \in R$ sont dit *congrus modulo* J, noté $a \equiv b \mod J$, s'ils appartiennent à la même classe résiduelle modulo J.

Définition 2.14. *L'ensemble des classes résiduelles d'un anneau R modulo un idéal J forme un anneau pour les opérations $(+ \mod J)$ et $(\cdot \mod J)$, c'est-à-dire les opérations de l'anneau R considérées modulo J. Cet anneau est appelé* anneau des classes résiduelles de R modulo J *et il est noté R/J.*

Théorème 2.15. *$\mathbb{Z}/(p)$, l'anneau des classes résiduelles des entiers modulo l'idéal principal engendré par un nombre premier p, est un corps.*

Les méthodes algébriques pour obtenir des règles de Golomb sont basées sur la construction de géométries sur des corps finis. Pour cette raison, nous nous intéressons maintenant à la caractérisation des corps finis. Les résultats suivants font ressortir le fait que tout corps fini est associé à un nombre premier, et inversement, que tout nombre premier peut être associé à un corps fini.

Définition 2.16. *Soit p un nombre premier. Le corps $\mathbb{Z}/(p)$ du théorème 2.15 est appelé* corps de Galois à p éléments *et il sera noté $\mathbb{F}_p$.*

Définition 2.17. *Si F est un corps et qu'il existe $n \in \mathbb{Z}$ tel que pour tout $r \in F$ on ait $nr = 0$, alors le plus petit entier positif satisfaisant cette propriété est appelé la* caractéristique *du corps F. S'il n'existe pas un tel entier positif, on dit que le corps F est de caractéristique 0.*

Théorème 2.18. *Tous les corps finis ont pour caractéristique un nombre premier.*

Polynômes à coefficients dans un corps

La notion de polynôme est au centre de la caractérisation des corps finis, principalement parce que tous les corps finis peuvent être vus comme des ensembles de polynômes. Nous présentons maintenant les différents résultats concernant les polynômes qui nous seront utiles plus tard afin de poursuivre la caractérisation des corps finis. Rappelons d'abord quelques termes généraux concernant les polynômes.

Un *polynôme* à coefficients dans un anneau R est une expression de la forme

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n,$$

où $n \in \mathbb{N}$, les a_i $(0 \leq i \leq n)$ appartiennent à R et x est un symbole appelé *l'indéterminé sur* R. Lorsqu'il n'y a pas de confusion pour l'indéterminé, nous noterons simplement f le polynôme $f(x)$. Le degré d'un polynôme f est le plus grand entier i tel que le coefficient a_i soit non nul ; de plus, si $a_i = 1$ alors on dit que f est un *polynôme monique*. Un polynôme non nul de degré 0 est appelé un *polynôme constant*.

Définition 2.19. *L'ensemble des polynômes à coefficients dans l'anneau R muni de l'addition et la multiplication usuelles pour les polynômes forme un anneau appelé* anneau des polynômes sur R *et noté $R[x]$. L'élément nul de $R[x]$ est le polynôme dont tous les coefficients sont égaux à 0 ; il est simplement noté 0.*

Le concept de division dans un anneau de polynômes $F[x]$, qui est central dans ce travail, nécessite que F soit un corps. Pour cette raison, dans le reste de ce texte, à moins de spécification contraire, nous ne considèrerons que des polynômes à coefficients dans un corps. Le théorème suivant introduit le concept de division pour les polynômes.

Théorème 2.20. *Soit F un corps et $g \neq 0$ un polynôme de $F[x]$. Alors pour tout $f \in F[x]$ il existe des polynômes $q, r \in F[x]$ tels que $f = qg + r$, où $\deg(r) < deg(g)$.*

Lorsque dans le théorème 2.20 le polynôme r est le polynôme nul, on dit que g *divise* f, sinon, on dit que r est le *reste de la division de f par g.*

Théorème 2.21. *Soit F un corps. Pour tout idéal $J \neq (0)$ de $F[x]$, il existe un polynôme monique uniquement déterminé $g \in F[x]$, tel que $J = (g)$.*

Définition 2.22. *Un polynôme $g \in F[x]$ est dit* irréductible sur F *si g a un degré non nul et que $g = pq$, avec $p, q \in F[x]$, implique que p ou q soit un polynôme constant.*

L'importance de la notion de polynôme irréductible pour la construction des corps finis provient du résultat suivant.

Théorème 2.23. *Soit f un polynôme de $F[x]$. L'anneau des classes résiduelles $F[x]/(f)$ est un corps si et seulement si f est irréductible sur F.*

Définition 2.24. *Un élément $b \in F$ est une* racine *du polynôme $f \in F[x]$ si $f(b) = 0$.*

Théorème 2.25. *Un élément $b \in F$ est une racine du polynôme $f \in F[x]$ si et seulement si $x - b$ divise $f(x)$.*

Extensions de corps

La structure de corps, comme les autres stuctures algébriques, admet la notion de sous-structure. Soit F un corps. Un sous-ensemble K de F qui est lui-même un corps pour les opérations de F est appelé un *sous-corps* de F ; dans ce cas, on dit aussi que F est une *extension* du corps K. Si $K \neq F$ on dit que K est un sous-corps *propre* de F.

Définition 2.26. *Un corps qui n'a pas de sous-corps propre est appelé un* corps premier.

L'intersection d'un nombre quelconque de sous-corps du corps F est aussi un sous-corps de F. L'intersection de tous les sous-corps de F est appelé le *sous-corps premier de F.*

Théorème 2.27. *Le sous-corps premier d'un corps fini F est isomorphe à $\mathbb{F}_p$, où p est la caractéristique du corps F.*

Étant donné un corps, il est possible de construire de nouveaux corps à partir de ce corps. Ces derniers sont appelés extensions du corps originel. Les prochains résultats, qui sont relatifs à la notion d'extension de corps, sont donc essentiels pour la caractérisation des corps finis.

Définition 2.28. *Soit K un sous-corps de F et M un sous-ensemble quelconque d'éléments de F. Le corps $K(M)$ défini par l'intersection de tous les sous-corps de F contenant K et M est appelé l'*extension de K par adjonction des éléments de M. *Si M est le singleton $\{\theta\} \subseteq F$, alors $L = K(\theta)$ est dite* extension simple de K *et θ est appelé* élément de définition de L sur K.

Définition 2.29. *Soit K un sous-corps de F et θ un élément de F. Si θ satisfait une équation polynomiale non triviale à coefficients dans K, c'est-à-dire, si $a_n\theta^n + \cdots + a_1\theta + a_0 = 0$ avec $a_n \neq 0$ pour $n > 0$, alors θ est dit* algébrique *sur le corps K. Une extension L du corps K est dite algébrique si tous les éléments de L sont algébriques sur le corps K.*

Définition 2.30. *Soit K un sous-corps de F et θ un élément de F. Si $\theta \in F$ est algébrique sur le corps K, alors l'unique polynôme monique $g \in K[x]$, par le théorème 2.21, qui génère l'idéal $\{f \in K[x] \mid f(\theta) = 0\}$ est appelé le* polynôme minimal *de θ sur K. On appelle* degré de θ sur K *le degré de g.*

Théorème 2.31. *Si $\theta \in F$ est algébrique sur le corps K, alors son polynôme minimal g sur K possède les propriétés suivantes :*

1. *g est irréductible dans $K[x]$.*
2. *Pour $f \in K[x]$ on a $f(\theta) = 0$ si et seulement si g divise f.*
3. *g est le polynôme monique de $K[x]$ de plus petit degré ayant θ pour racine.*

Remarque 2.32. *Si L est une extension du corps K, alors L peut être vu comme un espace vectoriel sur K. En effet, les éléments de L, qui sont des vecteurs d'éléments de K, forment un groupe abélien pour l'addition. Un élément $\alpha \in L$ peut être multiplié par un scalaire $r \in K$ de telle manière que $r\alpha$ soit également un élément de L et les lois pour la multiplication par un scalaire sont satisfaites, c'est-à-dire que pour $r, s \in K$ et $\alpha, \beta \in L$, on a*

1. $r(\alpha + \beta) = r\alpha + r\beta$,
2. $(r + s)\alpha = r\alpha + s\alpha$,

3. $(rs)\alpha = r(s\alpha)$, *et*

4. $1\alpha = \alpha$.

L est donc bien un espace vectoriel sur le corps K.

Dans ce qui suit, cette façon de voir les extensions de corps comme des espaces vectoriels sera souvent utilisée pour bien expliquer ce qui se passe.

Définition 2.33. *Soit L une extension d'un corps K. Si L, considéré comme un espace vectoriel sur K, est de dimension finie, alors L est appelée* extension finie du corps K. *La dimension de l'espace vectoriel L sur K est appelée* degré *de L sur K et notée $[L : K]$.*

Étant donné un corps K et un polynôme f sur ce corps, il est possible de construire un nouveau corps appelé corps de décomposition de f. Cette construction utilise le fait, tel que stipulé par le théorème ci-dessous, qu'il existe toujours une extension F du corps K telle que f puisse s'écrire comme produit de facteurs linéaires sur le corps $F[x]$. De façon plus formelle, on peut écrire ce qui suit.

Définition 2.34. *Soit $f \in K[x]$ de degré non nul et F une extension du corps K. Alors on dit que f se décompose dans F si f peut s'écrire comme produit de facteurs linéaires dans $F[x]$, c'est-à-dire s'il existe des éléments $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$ tels que*

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

où a est le coefficient de x^n dans le polynôme f. On dit aussi que F est le corps de décomposition de f sur K si f se décompose dans F et que $F = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Il est possible de parler *du corps* de décomposition d'un polynôme, puisque, comme le prochain résultat l'indique, ce corps est unique à isomorphisme près.

Théorème 2.35. *Si K est un corps et f un polynôme de degré non nul dans $K[x]$, alors il existe un corps de décomposition de f sur K. De plus, tous les corps de décomposition de f sur K sont isomorphes pour un isomorphisme qui fixe les éléments de K et envoie chaque racine de f sur une autre racine de f.*

Caractérisation des corps finis

Le prochain résultat implique que tous les sous-corps d'un corps fini de caractéristique p, en particulier le corps lui-même, ont une puissance de p comme cardinalité.

Théorème 2.36. *Soit F un corps fini. Alors F a p^n éléments, où p est un nombre premier qui est la caractéristique de F et n est le degré de F sur son sous-corps premier.*

Le lemme suivant est le dernier résultat nécessaire avant de pouvoir caractériser les corps finis. Ce lemme stipule que tout corps fini F peut être vu comme un corps de décomposition sur un sous-corps de F.

Lemme 2.37. *Si F est un corps fini qui contient q éléments et K est un sous-corps de F, alors le polynôme $x^q - x$ de $K[x]$ se factorise dans $F[x]$ comme*

$$x^q - x = \prod_{a \in F} (x - a)$$

et F est un corps de décomposition de $x^q - x$ sur K.

Le prochain résultat, appelé théorème de l'existence et de l'unicité des corps finis, caractérise entièrement les corps finis. Ce théorème stipule que pour toute puissance de nombre premier il existe un corps de cette cardinalité et que ce corps est unique à isomorphisme près.

Théorème 2.38. *Pour tout nombre premier p et tout entier naturel non nul n il existe un corps fini comportant p^n éléments. Tout corps fini comportant $q = p^n$ éléments est isomorphe au corps de décomposition de $x^q - x$ sur $\mathbb{F}_p$.*

Puisque tous les corps de décomposition sont isomorphes, il est alors possible de parler de l'unique corps fini de cardinalité p^n. Ce corps est noté $\mathbb{F}_{p^n}$ et il est appelé corps de Galois de cardinalité p^n.

Propriétés des corps finis

Pour un corps fini donné, il est possible de déterminer l'ensemble de ses sous-corps. Cette caractérisation pour les sous-corps est donnée par le théorème suivant.

Théorème 2.39. *Soit $q = p^n$ avec p premier et $n \geq 1$. Alors tous les sous-corps de $\mathbb{F}_q$ sont d'ordre p^m, où $m \geq 1$ est un diviseur de n. Inversement, si $m \geq 1$ est un diviseur de n, alors il existe un unique sous-corps de $\mathbb{F}_q$ avec p^m éléments.*

Dans ce qui suit, étant donné un corps fini $\mathbb{F}_q$, nous noterons $\mathbb{F}_q^*$ le groupe multiplicatif des éléments non nuls de $\mathbb{F}_q$. Le théorème suivant est une propriété des corps finis qui nous sera très utile.

Théorème 2.40. *Pour tout corps fini $\mathbb{F}_q$ le groupe multiplicatif $\mathbb{F}_q^*$ est cyclique.*

Définition 2.41. *Un générateur du groupe cyclique $\mathbb{F}_q^*$ est appelé un* élément primitif *de $\mathbb{F}_q$.*

Pour tout corps $\mathbb{F}_q$, il existe toujours un élément primitif. Ce fait implique, tel qu'indiqué par le théorème ci-dessous, que tout corps fini peut être vu comme une extension simple algébrique de son sous-corps premier.

Théorème 2.42. *Soit $\mathbb{F}_r$ une extension finie du corps $\mathbb{F}_q$. Alors $\mathbb{F}_r$ est une extension simple algébrique de $\mathbb{F}_q$ et n'importe quel élément primitif de $\mathbb{F}_r$ peut servir comme élément de définition de $\mathbb{F}_r$ sur $\mathbb{F}_q$.*

Corps de polynômes

Comme nous l'avons déjà vu, tous les corps finis peuvent être vus comme des corps de polynômes. Nous présentons maintenant quelques résultats concernant ces corps

de polynômes. En particulier, les prochains résultats nous permettent d'introduire la notion de polynôme primitif qui est nécessaire pour la construction des géométries finies.

Le lemme suivant est nécessaire pour nous permettre de définir l'ordre d'un polynôme.

Lemme 2.43. *Soit $f \in \mathbb{F}_q[x]$ un polynôme de degré $m \geq 1$ avec $f(0) \neq 0$. Alors il existe un entier naturel $e \leq q^m - 1$ tel que $f(x)$ divise $x^e - 1$.*

Définition 2.44. *Soit $f \in \mathbb{F}_q[x]$ un polynôme non nul. Si $f(0) \neq 0$, alors le plus petit entier e pour lequel $f(x)$ divise $x^e - 1$ est appelé l'*ordre de *f, noté $ord(f)$. Si $f(0) = 0$, alors $f(x)$ est de la forme $x^n g(x)$, où $n \in \mathbb{N}$ et $g \in \mathbb{F}_q[x]$ avec $g(0) \neq 0$. $ord(f)$ est alors défini comme $ord(g)$.*

Proposition 2.45. *Soit f un polynôme de degré m, irréductible dans $\mathbb{F}_q[x]$. Alors le corps de décomposition de f sur $\mathbb{F}_q$ est le corps $\mathbb{F}_{q^m}$.*

Théorème 2.46. *Soit $f \in \mathbb{F}_q[x]$ un polynôme irréductible sur $\mathbb{F}_q$ de degré $m \geq 1$ avec $f(0) \neq 0$. Alors $ord(f)$ est égal à l'ordre de n'importe quelle racine de f dans le groupe multiplicatif $\mathbb{F}_{q^m}^*$.*

Définition 2.47. *Un polynôme $f \in \mathbb{F}_q[x]$ de degré $m \geq 1$ est un* polynôme primitif sur $\mathbb{F}_q$ *s'il est le polynôme minimal sur $\mathbb{F}_q$ d'un élément primitif de $\mathbb{F}_{q^m}$.*

Théorème 2.48. *Un polynôme $f \in \mathbb{F}_q[x]$ de degré $m \geq 1$ est un* polynôme primitif sur $\mathbb{F}_q$ *si et seulement si f est monique, $f(0) \neq 0$, et $ord(f) = q^m - 1$.*

2.3.2 Géométries finies

La notion de géométrie finie construite sur un corps de Galois est centrale dans ce qui suit. La définition générale d'une géométrie projective de dimension m est présentée ci-après. Nous verrons ensuite des méthodes équivalentes de construction de ces espaces à partir d'un corps de Galois. Ces différentes constructions seront également illustrées à l'aide d'exemples.

Géométries projectives

Définition 2.49. *Un* plan projectif *ou un* espace projectif de dimension 2 *est constitué d'un ensemble de points, d'une famille de sous-ensembles particuliers de points, appelés droites, et d'une relation d'incidence entre les points et les droites satisfaisant les conditions suivantes :*

1. *chaque paire de droites distinctes est incidente à un seul point ;*
2. *chaque paire de points distincts est incidente à une seule droite ;*
3. *il existe quatre points tels qu'aucun ensemble de trois de ces points n'est incident à une même droite.*

Cette définition implique que chaque droite contient au moins trois points et que par chaque point il passe au moins trois droites.

Comme l'indique la définition suivante, le concept de plan projectif peut se généraliser aux espaces projectifs de dimension supérieure à 2.

Définition 2.50. *Une* géométrie projective de dimension m, *ou un* espace projectif de dimension m, *pour* $m \geq 2$, *est la donnée d'un ensemble de points et de droites satisfaisant les conditions de la définition précédente et de tous les sous-espaces de dimension* μ *pour* $2 \leq \mu < m$. *Les sous-espaces de dimension* μ *se définissent récursivement de la manière suivante. Les 0-espaces sont les points et les 1-espaces sont les droites. Si* $A_0, ..., A_\mu$, $2 \leq \mu < m$, *sont des points n'appartenant pas au même* $(\mu - 1)$*-espace, alors tous les points colinéaires avec* A_0 *et n'importe quel point du* $(\mu - 1)$*-espace défini par* $A_1, ..., A_\mu$ *forment un* μ*-espace. Ainsi, pour* $2 \leq \mu < m$ *tous les sous-espaces de dimension* μ *peuvent être déterminés de cette façon.*

L'espace vectoriel $\mathbb{F}_q^{k+1}$ induit une géométrie projective finie de dimension k qui sera notée $PG(k, \mathbb{F}_q)$. Soit $\mathcal{R}$ la relation d'équivalence sur les éléments non nuls de

$\mathbb{F}_q^{k+1}$ qui associe deux éléments à une même classe si et seulement si l'un est multiple de l'autre par un scalaire. Les points de $PG(k, \mathbb{F}_q)$ sont alors les classes d'équivalence de $\mathcal{R}$. Puisque le nombre de $(k+1)$-tuples non nuls sur le corps $\mathbb{F}_q$ est $q^{k+1}-1$ et que le nombre de scalaires non nuls est $q-1$, le nombre de points de $PG(k, \mathbb{F}_q)$ est

$$\frac{q^{k+1}-1}{q-1}.$$

Nous définissons ensuite un μ-espace (μ-flat) comme l'ensemble des points satisfaisant $k-\mu$ équations homogènes linéairement indépendantes :

$$\begin{array}{ccc} a_{10}x_0+ & \cdots & +a_{1k}x_k = 0 \\ a_{20}x_0+ & \cdots & +a_{2k}x_k = 0 \\ \vdots & & \vdots \\ a_{k-\mu,0}x_0+ & \cdots & +a_{k-\mu,k}x_k = 0 \end{array}$$

où les coefficients $a_{ij} \in \mathbb{F}_q$. Le nombre de points dans un sous-espace de dimension μ est alors

$$\frac{q^{\mu+1}-1}{q-1}.$$

En particulier, le plan projectif obtenu de cette manière sera noté $PG(2, \mathbb{F}_q)$.

Exemple 2.51. *Considérons l'espace vectoriel $\mathbb{F}_3^3$, puis construisons $PG(2, \mathbb{F}_3)$ de la manière indiquée ci-dessus. La relation $\mathcal{R}$ appliquée aux éléments non nuls de $\mathbb{F}_3^3$ nous donne les 13 points suivants :*

$$\begin{array}{rcl} (0,0,1) & \equiv & (0,0,2) \\ (0,1,0) & \equiv & (0,2,0) \\ (0,1,1) & \equiv & (0,2,2) \\ (0,1,2) & \equiv & (0,2,1) \\ (1,0,0) & \equiv & (2,0,0) \\ (1,0,1) & \equiv & (2,0,2) \\ (1,0,2) & \equiv & (2,0,1) \\ (1,1,0) & \equiv & (2,2,0) \\ (1,1,1) & \equiv & (2,2,2) \\ (1,1,2) & \equiv & (2,2,1) \\ (1,2,0) & \equiv & (2,1,0) \\ (1,2,1) & \equiv & (2,1,2) \\ (1,2,2) & \equiv & (2,1,1). \end{array}$$

Pour déterminer les 1-espaces, c'est-à-dire les droites, il faut maintenant considérer l'ensemble des points satisfaisant une équation homogène. L'équation $a_1x_1 + a_2x_2 + a_3x_3 = 0$ *étant simplement notée* $[a_1, a_2, a_3]$*, on obtient alors les 13 droites ci-dessous correspondant aux 13 équations homogènes distinctes possibles, et les points qui les composent.*

$$
\begin{array}{lllll}
[0,0,1]: & (0,1,0) & (1,0,0) & (1,1,0) & (1,2,0) \\
[0,1,0]: & (0,0,1) & (1,0,0) & (1,0,1) & (1,0,2) \\
[0,1,1]: & (0,1,2) & (1,0,0) & (1,1,2) & (1,2,1) \\
[0,1,2]: & (0,1,1) & (1,0,0) & (1,1,1) & (1,2,2) \\
[1,0,0]: & (0,0,1) & (0,1,0) & (0,1,1) & (0,1,2) \\
[1,0,1]: & (0,1,0) & (1,0,2) & (1,1,2) & (1,2,2) \\
[1,0,2]: & (0,1,0) & (1,0,1) & (1,1,1) & (1,2,1) \\
[1,1,0]: & (0,0,1) & (1,2,0) & (1,2,1) & (1,2,2) \\
[1,1,1]: & (0,1,2) & (1,0,2) & (1,1,1) & (1,2,0) \\
[1,1,2]: & (0,1,1) & (1,0,1) & (1,1,2) & (1,2,0) \\
[1,2,0]: & (0,0,1) & (1,1,0) & (1,1,1) & (1,1,2) \\
[1,2,1]: & (0,1,1) & (1,0,2) & (1,1,0) & (1,2,1) \\
[1,2,2]: & (0,1,2) & (1,0,1) & (1,1,0) & (1,2,2).
\end{array}
$$

Il est maintenant facile de vérifier que $PG(2, \mathbb{F}_3)$ *satisfait les conditions pour être un plan projectif.*

Soit α un élément primitif de $\mathbb{F}_{q^{k+1}}$. Alors les éléments non nuls de $\mathbb{F}_{q^{k+1}}$ s'expriment comme les puissances de α : $\alpha^0, \alpha^1, \ldots, \alpha^{q^{k+1}-2}$. Le théorème 2.39 implique que $\mathbb{F}_{q^{k+1}}$ a $\mathbb{F}_q$ comme sous-corps. Il existe donc un élément β de $\mathbb{F}_{q^{k+1}}$ d'ordre $q-1$ tel que $0, 1, \beta, \beta^2, \ldots, \beta^{q-2}$ forment le corps $\mathbb{F}_q$. Ainsi, les éléments non nuls de $\mathbb{F}_{q^{k+1}}$ peuvent également s'exprimer sous la forme $\beta^i\alpha^j$ pour $0 \leq i \leq q-2$ et $0 \leq j \leq \frac{q^{k+1}-1}{q-1} - 1$.

On peut donc aussi construire $PG(k, \mathbb{F}_q)$, à partir du corps $\mathbb{F}_{q^{k+1}}$, les points de $PG(k, \mathbb{F}_q)$ étant les $\frac{q^{k+1}-1}{q-1}$ ensembles $\{\beta^i\alpha^j \mid 0 \leq i \leq q-2\}$. Autrement dit, pour tous i et i', $0 \leq i, i' \leq q-2$, on identifie les éléments $\beta^i\alpha^j$ et $\beta^{i'}\alpha^j$, en prenant un

représentant de chaque classe on obtient alors les $\frac{q^{k+1}-1}{q-1}$ points de $PG(k, \mathbb{F}_q)$. Notons $\overline{\alpha^j}$ le représentant de la classe $\{\beta^i \alpha^j \mid 0 \leq i \leq q-2\}$. Pour former un μ-espace il suffit alors de prendre $\overline{\alpha^{i_0}}, \overline{\alpha^{i_1}}, \ldots, \overline{\alpha^{i_\mu}}$, $\mu+1$ points linéairement indépendants dans $PG(k, \mathbb{F}_q)$, et toutes les combinaisons linéaires $a_0\overline{\alpha^{i_0}} + a_1\overline{\alpha^{i_1}} + \ldots + a_\mu\overline{\alpha^{i_\mu}}$, avec $a_i \in \mathbb{F}_q$ non tous nuls, définissent alors un μ-espace (Lidl et Niederreiter, 1994). Ce qui vient d'être dit est illustré par l'exemple suivant.

Exemple 2.52. *Reprenons l'exemple 2.51, c'est-à-dire construisons $PG(2, \mathbb{F}_3)$. Sur le corps $\mathbb{F}_3 = (\{0,1,2\}, +, *)$, le seul élément primitif possible est 2. Pour effectuer les calculs, on détermine d'abord un polynôme primitif (voir remarque 2.66), c'est-à-dire satisfaisant les conditions du théorème 2.48, disons*

$$x^3 + 2x^2 + x + 1.$$

On prend ensuite une racine α du polynôme x^3+2x^2+x+1, nous donnant la relation

$$\alpha^3 = \alpha^2 + 2\alpha + 2.$$

On obtient alors pour points de la géométrie les points suivants.

$$\begin{array}{ll} \alpha^0 = 1 & \alpha^7 = \alpha^2 + \alpha \\ \alpha^1 = \alpha & \alpha^8 = \alpha^2 + \alpha + 1 \\ \alpha^2 = \alpha^2 & \alpha^9 = \alpha^2 + 1 \\ \alpha^3 = \alpha^2 + 2\alpha + 2 & \alpha^{10} = \alpha^2 + 2 \\ \alpha^4 = \alpha + 2 & \alpha^{11} = \alpha^2 + \alpha + 2 \\ \alpha^5 = \alpha^2 + 2\alpha & \alpha^{12} = \alpha^2 + 2\alpha + 1 \\ \alpha^6 = \alpha + 1. & \end{array}$$

Pour construire les 1-espaces, c'est-à-dire les droites, il suffit maintenant de considérer successivement les paires de points linéairement indépendants. On obtient de cette manière les droites suivantes :

$$
\begin{array}{lcllll}
1, \alpha & : & 1 & \alpha & \alpha^4 & \alpha^6 \\
1, \alpha^2 & : & 1 & \alpha^2 & \alpha^9 & \alpha^{10} \\
1, \alpha^3 & : & 1 & \alpha^3 & \alpha^5 & \alpha^{12} \\
1, \alpha^7 & : & 1 & \alpha^7 & \alpha^8 & \alpha^{11} \\
\alpha, \alpha^2 & : & \alpha & \alpha^2 & \alpha^5 & \alpha^7 \\
\alpha, \alpha^3 & : & \alpha & \alpha^3 & \alpha^{10} & \alpha^{11} \\
\alpha, \alpha^8 & : & \alpha & \alpha^8 & \alpha^9 & \alpha^{12} \\
\alpha^2, \alpha^3 & : & \alpha^2 & \alpha^3 & \alpha^6 & \alpha^8 \\
\alpha^2, \alpha^4 & : & \alpha^2 & \alpha^4 & \alpha^{11} & \alpha^{12} \\
\alpha^3, \alpha^4 & : & \alpha^3 & \alpha^4 & \alpha^7 & \alpha^9 \\
\alpha^4, \alpha^5 & : & \alpha^4 & \alpha^5 & \alpha^8 & \alpha^{10} \\
\alpha^5, \alpha^6 & : & \alpha^5 & \alpha^6 & \alpha^9 & \alpha^{11} \\
\alpha^6, \alpha^7 & : & \alpha^6 & \alpha^7 & \alpha^{10} & \alpha^{12}.
\end{array}
$$

Encore une fois, il est facile de vérifier que cette construction satisfait tous les axiomes d'une géométrie projective, et par conséquent que les deux constructions proposées sont équivalentes.

Remarque 2.53. *La correspondance entre les points et les droites d'un plan projectif obtenus par la méthode de l'exemple 2.51 et ceux obtenus par la méthode de l'exemple précédent peut se faire de la manière suivante. Le point* $\alpha^j = \beta_2\alpha^2+\beta_1\alpha+\beta_0$, $\beta_i \in \mathbb{F}_q$, $i = 0, 1, 2$, *correspond bijectivement au point* $(\beta_2, \beta_1, \beta_0)$ *de l'exemple 2.51. La droite associée à deux points distincts* $\alpha^{j_1} = \beta_{1,2}\alpha^2+\beta_{1,1}\alpha+\beta_{1,0}$ *et* $\alpha^{j_2} = \beta_{2,2}\alpha^2+\beta_{2,1}\alpha+\beta_{2,0}$, $\beta_{i,j} \in \mathbb{F}_q$, $i = 1, 2$ *et* $j = 0, 1, 2$, *correspond bijectivement à l'unique droite* $[\beta_2, \beta_1, \beta_0]$ *de l'exemple 2.51 satisfaisant*

$$\beta_2\beta_{1,2} + \beta_1\beta_{1,1} + \beta_0\beta_{1,0} = 0 \text{ et}$$

$$\beta_2\beta_{2,2} + \beta_1\beta_{2,1} + \beta_0\beta_{2,0} = 0.$$

Pour l'exemple 2.51 et l'exemple 2.52 la correspondance pour les points s'établit comme suit.

α^0	$=$					1	*(0,0,1)*
α^1	$=$			α			*(0,1,0)*
α^2	$=$	α^2					*(1,0,0)*
α^3	$=$	α^2	$+$	2α	$+$	2	*(1,2,2)*
α^4	$=$			α	$+$	2	*(0,1,2)*
α^5	$=$	α^2	$+$	2α			*(1,2,0)*
α^6	$=$			α	$+$	1	*(0,1,1)*
α^7	$=$	α^2	$+$	α			*(1,1,0)*
α^8	$=$	α^2	$+$	α	$+$	1	*(1,1,1)*
α^9	$=$	α^2	$+$			1	*(1,0,1)*
α^{10}	$=$	α^2	$+$			2	*(1,0,2)*
α^{11}	$=$	α^2	$+$	α	$+$	2	*(1,1,2)*
α^{12}	$=$	α^2	$+$	2α	$+$	1	*(1,2,1)*

De même, la correspondance pour les droites s'établit de la manière suivante.

$[0,0,1]:(0,1,0),(1,0,0),(1,1,0),(1,2,0)$	α,α^2	:	α	α^2	α^5	α^7
$[0,1,0]:(0,0,1),(1,0,0),(1,0,1),(1,0,2)$	$1,\alpha^2$	:	1	α^2	α^9	α^{10}
$[0,1,1]:(0,1,2),(1,0,0),(1,1,2),(1,2,1)$	α^2,α^4	:	α^2	α^4	α^{11}	α^{12}
$[0,1,2]:(0,1,1),(1,0,0),(1,1,1),(1,2,2)$	α^2,α^3	:	α^2	α^3	α^6	α^8
$[1,0,0]:(0,0,1),(0,1,0),(0,1,1),(0,1,2)$	$1,\alpha$	:	1	α	α^4	α^6
$[1,0,1]:(0,1,0),(1,0,2),(1,1,2),(1,2,2)$	α,α^3	:	α	α^3	α^{10}	α^{11}
$[1,0,2]:(0,1,0),(1,0,1),(1,1,1),(1,2,1)$	α,α^8	:	α	α^8	α^9	α^{12}
$[1,1,0]:(0,0,1),(1,2,0),(1,2,1),(1,2,2)$	$1,\alpha^3$	:	1	α^3	α^5	α^{12}
$[1,1,1]:(0,1,2),(1,0,2),(1,1,1),(1,2,0)$	α^4,α^5	:	α^4	α^5	α^8	α^{10}
$[1,1,2]:(0,1,1),(1,0,1),(1,1,2),(1,2,0)$	α^5,α^6	:	α^5	α^6	α^9	α^{11}
$[1,2,0]:(0,0,1),(1,1,0),(1,1,1),(1,1,2)$	$1,\alpha^7$	:	1	α^7	α^8	α^{11}
$[1,2,1]:(0,1,1),(1,0,2),(1,1,0),(1,2,1)$	α^6,α^7	:	α^6	α^7	α^{10}	α^{12}
$[1,2,2]:(0,1,2),(1,0,1),(1,1,0),(1,2,2)$	α^3,α^4	:	α^3	α^4	α^7	α^9

Plan semi-affine

Le plan projectif n'est pas le seul type de géométrie finie qui puisse être utilisé pour obtenir des règles de Golomb. À partir d'une géométrie projective, il est possible de construire une géométrie affine et, de celle-ci, obtenir une géométrie semi-affine. Le

plan semi-affine possède les mêmes propriétés pour l'obtention de règles de Golomb que le plan projectif. Dans ce qui suit, nous présentons une méthode pour obtenir le plan semi-affine à partir du plan projectif.

Étant donné le plan projectif $PG(2, \mathbb{F}_q)$, il existe plusieurs façons de construire un plan semi-affine. Toutefois, lorsque nous référerons au plan semi-affine, noté $SAP(\mathbb{F}_q)$, nous considérerons le plan obtenu par la construction suivante. À partir de $PG(2, \mathbb{F}_q)$, on construit le plan affine en enlevant une droite et les points incidents à cette droite (Lidl et Niederreiter, 1994). Puis, du plan affine, on enlève un point et les droites incidentes à ce point. Le plan ainsi obtenu est $SAP(\mathbb{F}_q)$, qui contient $q^2 - 1$ points et $q^2 - 1$ droites. Chaque droite contient q points et chaque point est incident à q droites (Coolsaet, n.d.).

Exemple 2.54. *Pour illustrer cette construction, considérons* $PG(2, \mathbb{F}_3)$ *construite à l'exemple 2.51. Sans perte de généralité, choisissons d'ôter la droite* $[0, 0, 1]$. *Tel qu'indiqué ci-dessus, il faut donc ôter les points* $(0, 1, 0)$, $(1, 0, 0)$, $(1, 1, 0)$ *et* $(1, 2, 0)$ *de chaque droite pour obtenir un plan affine. De ce plan, on choisit sans perte de généralité d'ôter le point* $(0, 0, 1)$. *Il faut alors ôter les droites* $[0, 1, 0]$, $[1, 0, 0]$, $[1, 1, 0]$ *et* $[1, 2, 0]$. *Il nous reste alors le plan semi-affine* $SAP(\mathbb{F}_3)$, *dont les points et les droites sont donnés dans le tableau ci-dessous.*

$SAP(\mathbb{F}_3)$				
Points	*Droites*			
(0,1,1)	*[0,1,1] :*	*(0,1,2)*	*(1,1,2)*	*(1,2,1)*
(0,1,2)	*[0,1,2] :*	*(0,1,1)*	*(1,1,1)*	*(1,2,2)*
(1,0,1)	*[1,0,1] :*	*(1,0,2)*	*(1,1,2)*	*(1,2,2)*
(1,0,2)	*[1,0,2] :*	*(1,0,1)*	*(1,1,1)*	*(1,2,1)*
(1,1,1)	*[1,1,1] :*	*(0,1,2)*	*(1,0,2)*	*(1,1,1)*
(1,1,2)	*[1,1,2] :*	*(0,1,1)*	*(1,0,1)*	*(1,1,2)*
(1,2,1)	*[1,2,1] :*	*(0,1,1)*	*(1,0,2)*	*(1,2,1)*
(1,2,2)	*[1,2,2] :*	*(0,1,2)*	*(1,0,1)*	*(1,2,2)*

On peut vérifier qu'il y a bien 8 *points et* 8 *droites, que chaque droite contient* 3 *points, et que chaque point est incident à* 3 *droites.*

Remarquons que le dernier élément de chaque point est non nul, et qu'il est toujours possible d'obtenir cette propriété, ce qui nous permet de construire directement le plan semi-affine à l'aide d'équations (non homogènes) comme pour le cas des droites projectives.

Récurrences linéaires

Définition 2.55. *Soit $s_0, s_1, s_2, \ldots$, une suite infinie d'éléments d'un corps satisfaisant la récurence linéaire d'ordre k suivante : $s_{n+k} = \sum_{i=1}^{k} a_{k-i} s_{n+k-i}$. Le* polynôme caractéristique *de cette suite est le polynôme $x^k - \sum_{i=1}^{k} a_{k-i} x^{k-i}$. La suite est dite* périodique de période p *si p est le plus petit entier vérifiant $s_{n+p} = s_n$ pour tout n. Toutes les suites ne sont naturellement pas périodiques; dans ce cas la période sera considérée comme étant infinie.*

L'exemple suivant illustre les notions que nous venons de définir.

Exemple 2.56. *Considérons la suite de Fibonacci, dont les premiers termes sont*

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots.$$

Cette suite est définie par la récurrence linéaire d'ordre deux $s_{n+2} = s_{n+1} + s_n$. Le polynôme caractéristique de cette suite est donc $x^2 - x - 1$. Puisque la suite est strictement croissante, elle ne peut pas être périodique (elle est donc de période ∞).

Considérons maintenant la même suite prise modulo 2. Les premiers termes sont alors

$$0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, \ldots.$$

Puisque l'on travaille modulo 2, le polynôme caractéristique de la suite peut s'écrire $x^2 - x - 1$ ou $x^2 + x + 1$, et la suite de Fibonacci prise modulo 2 est de période 3.

Étant donné une équation de récurrence d'ordre k sur le corps $\mathbb{F}_q$, donc un polynôme $f(x) \in \mathbb{F}_q[x]$ de degré k, la suite dont les conditions initiales sont 0 pour les $k-1$ premiers termes et 1 pour le k-ième terme est appelée *suite de réponses d'impulsion (impulse response sequence)*. Par exemple, la suite de Fibonacci modulo 2 de l'exemple 2.56 est la suite de réponses d'impulsion du polynôme $x^2+x+1 \in \mathbb{F}_2[x]$.

Remarque 2.57. *Le lecteur peut vérifier qu'étant donné un polynôme monique $f(x) \in \mathbb{F}_q[x]$ de degré k, les $ord(f)$ premiers termes de la suite de réponses d'impulsion de f correspondent aux coefficients du polynôme $g(x) \in \mathbb{F}_q[x]$ lorsque*

$$g(x) = \frac{x^{ord(f)} - 1}{f(x)}.$$

Notons que les $k-1$ coefficients des monômes de plus grand degré de $g(x)$ sont nuls. Cette remarque implique donc que de façon alternative, on peut définir un polynôme $f(x) \in \mathbb{F}_q[x]$ de degré k comme étant primitif sur $\mathbb{F}_q$ si et seulement si la suite de réponses d'impulsion est périodique de période $q^k - 1$.

Pour illustrer cette remarque, reprenons le polynôme x^3+2x^2+x+1 de $\mathbb{F}_3[x]$ de l'exemple 2.52.

Exemple 2.58. *Soit $f(x) = x^3 + 2x^2 + x + 1$ le polynôme caractéristique de la récurrence $s_{n+3} = -2s_{n+2} - s_{n+1} - s_n$. Puisque l'on travaille sur le corps $\mathbb{F}_3$, l'équation de récurrence s'écrit donc sous la forme $s_{n+3} = s_{n+2} + 2s_{n+1} + 2s_n$. Les 3^3-1 premiers termes de la suite de réponses d'impulsion de f sont donc*

$$0,0,1,1,0,1,0,2,1,2,2,2,1,0,0,2,2,0,2,0,1,2,1,1,1,2.$$

En appliquant l'algorithme de division d'Euclide avec $f(x)$ comme diviseur, on trouve que le plus petit entier e satisfaisant la condition que $f(x)$ divise $x^e - 1$ est $e = 26 = 3^3 - 1$, donc que f est primitif. On trouve alors que

$$x^{26}-1 = (x^3+2x^2+x+1)(0x^{25}+0x^{24}+1x^{23}+1x^{22}+0x^{21}+1x^{20}+0x^{19}+2x^{18}+1x^{17}$$

$$+2x^{16}+2x^{15}+2x^{14}+1x^{13}+0x^{12}+0x^{11}+2x^{10}+2x^9+0x^8+2x^7+0x^6+1x^5+2x^4+1x^3$$
$$+1x^2+1x^1+2x^0).$$

Ainsi, les coefficients du second polynôme de droite sont bien les premiers termes de la suite de réponses d'impulsion de f comme nous l'avons mentionné dans la remarque précédente.

Si f est un polynôme primitif de degré k sur le corps $\mathbb{F}_q$, nous noterons $S(f)$ la suite de réponses d'impulsion de f. Puisque la période de $S(f)$ est $q^k - 1$, tous les k-tuples d'éléments de $\mathbb{F}_q$ apparaissent dans $S(f)$. Nous noterons $POS_{S(f)} : (\mathbb{F}_q^k)^* \rightarrow \{0, 1, ..., q^k - 2\}$ la fonction qui associe à un k-tuple la position de sa première apparition dans $S(f)$. Lorsque f est primitif, $POS_{S(f)}$ est une bijection et par conséquent, elle induit un isomorphisme de corps entre $(\mathbb{F}_q^k)^*$ et $\mathbb{F}_{q^k}^*$.

CDS

Définition 2.59. *Un* CDS (Cyclic Difference Set) modulo n de taille s *est un ensemble, contenant* 0, *de* s *entiers positifs ou nuls* $\{a_1, a_2, ..., a_s\}$ *inférieurs à* n *tel que toutes les différences* $a_i - a_j \mod n$, *pour* $i \neq j$, *sont distinctes.*

Étant donné $\{a_1, a_2, ..., a_s\}$ un CDS modulo n, on appelle *décalage* de ce CDS n'importe quel ensemble de la forme

$$\{a_1 + i \mod n, a_2 + i \mod n, ..., a_s + i \mod n\},$$

pour $0 \leq i \leq n - 1$. En particulier, lorsque 0 apparaît dans le décalage, on a un nouveau CDS. Soit m un entier relativement premier avec n, où $m < n$. On définit un nouveau CDS modulo n en prenant l'ensemble

$$\{ma_1 \mod n, ma_2 \mod n, ..., ma_s \mod n\}.$$

Dans ce cas, l'entier m est appelé un *multiplicateur* du CDS (Coolsaet, n.d.). La notion de CDS est illustrée par l'exemple 2.60.

Exemple 2.60. *L'ensemble* $\{0,1,4,6\}$ *définit un CDS modulo 13 de taille 4 puisque les différences modulo 13 engendrées sont toutes distinctes, tel qu'illustré ci-dessous.*

$$\begin{array}{lll} 0-1\equiv 12 \mod 13, & 0-4\equiv 9 \mod 13, & 0-6\equiv 7 \mod 13, \\ 1-0\equiv 1 \mod 13, & 1-4\equiv 10 \mod 13, & 1-6\equiv 8 \mod 13, \\ 4-0\equiv 4 \mod 13, & 4-1\equiv 3 \mod 13, & 4-6\equiv 11 \mod 13, \\ 6-0\equiv 6 \mod 13, & 6-1\equiv 5 \mod 13, & 6-4\equiv 2 \mod 13. \end{array}$$

L'ensemble $\{7,8,11,0\}$ *est un décalage du CDS de départ, obtenu en additionnant* 7 mod 13 *à tous les éléments. Notons que ce décalage forme également un CDS modulo 13 de taille 4. Puisque 3 est relativement premier à 13, 3 est un multiplicateur du CDS de départ. Le nouveau CDS, obtenu en multipliant chaque élément par 3, est alors* $\{0,3,12,5\}$. *Dans les deux cas précédents, il est facile de vérifier que les ensembles obtenus sont bien des CDS.*

Remarque 2.61. *Étant donné un ensemble formant un CDS, cet ensemble définit également une règle de Golomb. Cette observation, bien qu'évidente, est essentielle dans ce qui suit, puisque les règles de Golomb que nous construirons seront toujours induites par des CDS.*

En considérant $\{a_1 = 0, a_2, ..., a_s\}$ un CDS modulo $n = s^2 - s + 1$ de taille s et l'ensemble de ses décalages

$$\{\{a_1 + i \mod n, a_2 + i \mod n, ..., a_s + i \mod n\} \mid 0 \leq i \leq n-1\},$$

on voit que chaque paire d'entiers apparaît dans exactement un décalage et que deux décalages possèdent exactement un entier en commun. La structure de plan projectif est donc appropriée à la construction d'ensembles formant des CDS, où les entiers sont associés aux points et les décalages aux droites du plan projectif (Coolsaet, n.d.). L'exemple suivant illustre cette affirmation.

Exemple 2.62. *Reprenons le CDS* $\{0,1,4,6\}$ mod 13 *de l'exemple 2.60. L'ensemble*

des décalages induits par ce CDS est :

0	1	4	6	mod 13
1	2	5	7	
2	3	6	8	
3	4	7	9	
4	5	8	10	
5	6	9	11	
6	7	10	12	
7	8	11	0	
8	9	12	1	
9	10	0	2	
10	11	1	3	
11	12	2	4	
12	0	3	5	

On peut vérifier qu'avec les entiers modulo 13 comme points et les décalages comme droites, cette structure satisfait les axiomes du plan projectif de la définition 2.49.

2.3.3 Algorithme pour les règles de Golomb

Dans cette section, nous présentons un algorithme pour la construction des CDS. Cet algorithme combine des méthodes de construction du plan projectif, introduit par Singer (1938), et du plan semi-affine, introduit par Bose (1942). L'idée de construction des règles de Golomb à partir de CDS, qui a été introduite dans les années 1980 (Atkinson et al., 1986; Lam et Sarwate, 1988), donne encore, à ce jour, les meilleurs résultats connus pour la construction des règles de Golomb avec un grand nombre de marques. Pour cette raison, nous voulons adapter ces méthodes algébriques au cas des ensembles doublement orthogonaux. La formulation de l'algorithme et les détails s'y rattachant sont donc présentés sous une forme qui pourra facilement être généralisée au cas qui nous intéresse.

Construction du plan projectif

Pour construire le plan projectif $PG(2, \mathbb{F}_q)$, nous utilisons la notion de récurrence linéaire. Rappelons qu'un polynôme caractéristique primitif f de degré 3 engendre une suite $S(f)$ de période $q^3 - 1$. Ainsi, les $q^3 - 1$ premiers éléments de $S(f)$ forment tous les triplets non nuls d'éléments de $\mathbb{F}_q$. Le résultat suivant nous assure qu'il est suffisant de considérer seulement les $\frac{q^3-1}{q-1}$ premiers triplets de $S(f)$ pour représenter les points du plan projectif.

Proposition 2.63. *(Singer, 1938) Parmi les $\frac{q^3-1}{q-1}$ premiers triplets de $S(f)$, aucun triplet n'est multiple d'un autre par un scalaire.*

Preuve. Soient $u = (u_0, u_1, u_2)$ et $v = (\beta u_0, \beta u_1, \beta u_2)$, $\beta \in \mathbb{F}_q$, deux triplets tels que $POS_{S(f)}(u) - POS_{S(f)}(v) < \frac{q^3-1}{q-1}$. Notons p l'ordre de β dans $\mathbb{F}_q$. La seconde apparition du triplet u dans $S(f)$ est donc, au plus, à la position $p * (POS_{S(f)}(u) - POS_{S(f)}(v))$, mais puisque p est nécessairement inférieur ou égal à $q - 1$, la période de $S(f)$ doit être strictement inférieure à $q^3 - 1$, ce qui est une contradiction. Par conséquent, deux triplets multiples par un scalaire ne peuvent pas être tous les deux présents parmi les $\frac{q^3-1}{q-1}$ premiers triplets de $S(f)$.

□

La proposition 2.63 et le fait que $PG(2, \mathbb{F}_q)$ contient $\frac{q^3-1}{q-1}$ points nous permettent de dire que les $\frac{q^3-1}{q-1}$ premiers triplets de $S(f)$ formeront les points de $PG(2, \mathbb{F}_q)$. Pour définir les droites, nous dirons que deux points $u = (u_0, u_1, u_2)$ et $v = (v_0, v_1, v_2)$, pour des $u_i, v_i \in \mathbb{F}_q$, appartiennent à une même droite si et seulement si u et v satisfont la même équation linéaire homogène (Lidl et Niederreiter, 1994).

Étant donné un plan projectif construit par la méthode énoncée ci-dessus, le résultat suivant nous indique la façon dont les CDS en sont déduits.

Proposition 2.64. *(Singer, 1938) Soit* $\{p_0 = (0,0,1), p_1, \ldots, p_q\}$ *un ensemble de* $q+1$ *triplets formant une droite dans* $PG(2,\mathbb{F}_q)$*, construit par la méthode énoncée ci-dessus. L'ensemble*

$$\{POS_{S(f)}(p_i) \mid 0 \leq i \leq q\}$$

forme un CDS modulo $\frac{q^3-1}{q-1}$ *de taille* $q+1$.

Preuve. On a $POS_{S(f)}(p_0) = 0$. Considérons les $q+1$ droites contenant le point p_0. Chacune de ces droites contient q points distincts des points des autres droites puisque dans $PG(2,\mathbb{F}_q)$ deux droites s'intersectent en exactement un point. Comme nous l'avons vu, il est possible de voir les points de $PG(2,\mathbb{F}_q)$ comme les puissances de α, un élément primitif de $\mathbb{F}_{q^3}$. Puisque f est primitif, $POS_{S(f)}$ induit une bijection entre $(\mathbb{F}_q^3)^*$ et $\mathbb{F}_{q^3}^*$. En effet, il suffit de fixer $POS^{-1}_{S(f)}(\ell) = \alpha^\ell$. Ainsi, à partir de la droite $\{p_0, p_1, ..., p_q\}$, on peut construire toutes les droites de $PG(2,\mathbb{F}_q)$ en prenant

$$\{\{\alpha^{POS_{S(f)}(p_i)+j} \mid 0 \leq i \leq q\} \mid 0 \leq j \leq \frac{q^3-q}{q-1}\}.$$

Ceci implique que $\{POS_{S(f)}(p_i) \mid 0 \leq i \leq q\}$ forme un CDS modulo $\frac{q^3-1}{q-1}$ de taille $q+1$.

□

Remarque 2.65. *Pour illustrer la proposition 2.64, il suffit de comparer l'ensemble des droites obtenues dans l'exemple 2.52 à l'ensemble des décalages obtenus dans l'exemple 2.62. Il est alors facile de vérifier que chaque ensemble de puissances de la racine primitive* α *formant une droite dans* $PG(2,\mathbb{F}_3)$ *correspond à un décalage pour le CDS* $\{0,1,4,6\}$ mod 13*, et vice versa.*

Algorithme pour le plan projectif

L'algorithme que nous proposons consiste simplement à déterminer le plus grand nombre de droites projectives dont chacune induit un CDS. Or, nous venons de voir

que chaque droite de $PG(2, \mathbb{F}_q)$ contenant le point $p_0 = (0, 0, 1)$ induit un CDS modulo $\frac{q^3-1}{q-1}$. Toutefois, pour obtenir toutes ces droites, une seule suffira, puisque, comme nous l'avons vu, chaque droite correspond alors à un décalage. Notre algorithme devra donc considérer tous les décalages induisant un nouveau CDS. Aussi, comme nous l'avons déjà mentionné, les multiplicateurs peuvent également fournir de nouveaux CDS. Cette opération devra donc aussi être appliquée dans notre algorithme.

Nous sommes maintenant en mesure de formuler brièvement le pseudo-code de l'algorithme en ce qui concerne la technique du plan projectif.

Algorithme 2.1 Obtention du meilleur CDS à partir de $PG(2, q)$

Antécédent: q une puissance de nombre premier
Conséquent: $\mathcal{C}$ un CDS de longueur minimale correspondant à une droite de $PG(2, q)$

1: Déterminer un polynôme primitif f sur $\mathbb{F}_q$ de degré 3
2: Construire la suite $S(f)$
3: Trouver une droite D contenant le point (0,0,1)
4: Convertir D en ensemble d'entiers E avec la fonction $POS_{S(f)}$
5: **pour** $i = 0$ **à** $\frac{q^3-1}{q-1} - 1$ **faire**
6: **si** $\frac{q^3-1}{q-1} - i \in E$ **alors**
7: **pour** $j = 1$ **à** $\frac{q^3-1}{q-1} - 1$ **faire**
8: **si** $(\frac{q^3-1}{q-1} - 1, j) = 1$ **alors**
9: Appliquer le multiplicateur j sur E avec décalage de i
10: **si** $\mathcal{C}$ est de longueur supérieur à la nouvelle droite **alors**
11: affecter la nouvelle droite à $\mathcal{C}$
12: **fin si**
13: **fin si**
14: **fin pour**
15: **fin si**
16: **fin pour**
17: **retourner** $\mathcal{C}$

Les trois premières étapes de cet algorithme consistent à déterminer une droite du plan projectif qui contient le point $(0, 0, 1)$. La condition que le point $(0, 0, 1)$ appartienne à la droite a pour but que l'élément 0 appartienne au CDS que nous

construisons à la ligne 4. Les lignes 5 à 9 consistent à trouver tous les CDS possibles avec les multiplicateurs et les décalages. À chaque nouveau CDS obtenu on vérifie si la longueur du CDS a diminué et on mémorise le CDS de longueur minimale, ce qui correspond à la ligne 10. Finalement, la ligne 17 consiste à retourner le dernier CDS mémorisé, c'est-à-dire le CDS de longueur minimale.

Remarque 2.66. *Pour déterminer un polynôme primitif, on considère successivement les polynômes moniques $f \in \mathbb{F}_q[x]$ de degré 3, jusqu'à l'obtention d'une suite $S(f)$ de période $q^3 - 1$. Le théorème 2.40, qui assure l'existence d'un polynôme primitif, et le fait que le nombre de polynômes de degré 3 dans $\mathbb{F}_q[x]$ est fini impliquent qu'un polynôme primitif sera toujours obtenu de cette manière. Les étapes 1 et 2 de l'algorithme peuvent donc se traduire par : trouver $f \in \mathbb{F}_q[x]$ de degré 3 tel que $S(f)$ est de période $q^3 - 1$.*

Puisque le nombre de polynômes moniques de dégré 3 dans $\mathbb{F}_q[x]$ appartient à $\mathcal{O}(q^3)$ et qu'il faut considérer des suites de longueur appartenant à $\mathcal{O}(q^3)$ pour déterminer si un polynôme est primitif, la recherche d'un polynôme primitif se fait donc dans un temps appartenant à $\mathcal{O}(q^9)$. Toutes les autres étapes de l'algorithme 2.1 s'effectue dans des temps inclus dans $\mathcal{O}(q^9)$, y compris la boucle débutant à la ligne 5 qui appartient à $\mathcal{O}(q^4)$. Donc de façon générale, la complexité de l'algorithme 2.1 correspond à la complexité de trouver un polynôme primitif, c'est-à-dire qu'elle appartient à $\mathcal{O}(q^9)$.

Construction du plan semi-affine

Considérons maintenant le plan semi-affine $SAP(\mathbb{F}_q)$. Construisons $SAP(\mathbb{F}_q)$ en enlevant la droite de $PG(2, \mathbb{F}_q)$ correspondant à l'équation linéaire $x_3 = 0$ et tous les points incidents à cette droite, c'est-à-dire en enlevant tous les triplets dont la dernière composante est 0. Puis enlevons le point $(0, 0, 1)$ et les droites incidentes à ce point. $SAP(\mathbb{F}_q)$ contient alors $q^2 - 1$ droites et $q^2 - 1$ points. Puisque dans $PG(2, \mathbb{F}_q)$

les multiples d'un triplet sont équivalents, il est possible de représenter les points par les triplets ayant leur dernière composante non nulle égale à 1. L'ensemble des points de $SAP(\mathbb{F}_q)$ peut alors être représenté par les couples non nuls d'éléments de $\mathbb{F}_q$ auxquels on ajoute une troisième composante égale à 1. Les droites sont formées sous les mêmes conditions que pour $PG(2, \mathbb{F}_q)$ en ne prenant que les équations linéaires telles que $a_3 = q - 1$ et $a_1 \neq 0$ ou $a_2 \neq 0$. Autrement dit, on peut voir les points de $SAP(\mathbb{F}_q)$ comme les couples non nuls de $\mathbb{F}_q^2$, et alors, une droite de $SAP(\mathbb{F}_q)$ est formée des couples (x_1, x_2) satisfaisant une équation linéaire de la forme

$$a_1 x_1 + a_2 x_2 = 1,$$

pour $a_1, a_2 \in \mathbb{F}_q$, non tous deux nuls. Par construction, $SAP(\mathbb{F}_q)$ possède les mêmes propriétés que $PG(2, \mathbb{F}_q)$ pour l'obtention de CDS. On obtient alors des CDS modulo $q^2 - 1$ de taille q.

Exemple 2.67. *Pour illustrer ce qui vient d'être dit, il suffit de comparer le plan semi-affine défini ci-dessous et celui construit à l'exemple 2.54 pour voir qu'il y a bien un isomorphisme entre les deux plans.*

$SAP(\mathbb{F}_3)$				
Points	*Droites*			
(0,2)	*[0,2] :*	*(0,2)*	*(1,2)*	*(2,2)*
(0,1)	*[0,1] :*	*(0,1)*	*(1,1)*	*(2,1)*
(2,0)	*[2,0] :*	*(2,0)*	*(2,1)*	*(2,2)*
(1,0)	*[1,0] :*	*(1,0)*	*(1,1)*	*(1,2)*
(2,2)	*[2,2] :*	*(0,2)*	*(1,1)*	*(2,0)*
(1,1)	*[1,1] :*	*(0,1)*	*(1,0)*	*(2,2)*
(2,1)	*[2,1] :*	*(0,1)*	*(1,2)*	*(2,0)*
(1,2)	*[1,2] :*	*(0,2)*	*(1,0)*	*(2,1)*

Algorithme pour le plan semi-affine

Pour convertir l'algorithme présenté dans le cas du plan projectif en un algorithme pour $SAP(\mathbb{F}_q)$, des modifications mineures sont suffisantes : à l'étape 1, on détermine

un polynôme primitif de degré 2 ; à l'étape 3, on trouve à partir de $S(f)$ une droite contenant le point $(0, 1)$; le reste de l'algorithme est identique.

Remarque 2.68. *La remarque 2.66 s'applique également à ce cas-ci, à la différence que le polynôme f cherché doit être de degré 2, et que $S(f)$ doit alors être de période $q^2 - 1$.*

Remarques relatives aux constructions

La construction des plans projectifs et semi-affines se fait à partir d'un corps fini $\mathbb{F}_q$; par conséquent, le nombre de marques pour les règles de Golomb obtenues est toujours relatif à q, une puissance d'un nombre premier. Pour construire une règle de Golomb avec M marques, où M est différent d'un nombre premier, on considère des CDS de tailles supérieures et on leur enlève le nombre de marques requis. De plus, a priori, rien n'empêche que l'on puisse obtenir une meilleure règle de Golomb avec un CDS de taille supérieure à M. Ainsi, pour obtenir les meilleurs résultats possibles pour une règle de Golomb avec M marques, on fixe d'abord un entier t, puis on construit toutes les règles possibles à partir de $SAP(\mathbb{F}_q)$ et de $PG(2, \mathbb{F}_q)$, avec $M \leq q \leq M + t$, pour q une puissance d'un nombre premier.

2.3.4 Résultats numériques

Dans cette section nous voulons présenter les différents résultats obtenus pour les implémentations de l'algorithme 2.1 et son équivalent pour le plan semi-affine. Nous voulons d'une part, montrer l'efficacité de l'algorithme 2.1 en terme de la longueur des règles de Golomb obtenues, et d'autre part, montrer la capacité de déterminer des règles de bonne qualité pour des ordres qui ne peuvent être atteints qu'avec les méthodes algébriques.

Nous comparons dans le Tableau 2.2 les longueurs des règles de Golomb obtenues par notre algorithme par rapport aux règles de Golomb obtenues par une méthode de recherche tabou présentée par Galinier et Jaumard (2006) et par rapport aux règles de Golomb dont l'optimalité est connue. Mentionnons que la méthode de Galinier et Jaumard est avec l'algorithme GARSP, que nous avons présenté précédemment, parmi les meilleures méthodes pour prouver l'optimalité des règles de Golomb. Les heuristiques issues de la résolution partielle des ces algorithmes donnent des résultats qui peuvent être comparés en termes de longueur des règles avec l'algorithme 2.1, mais en terme de temps de calcul, il n'y a pas de comparaison possible puisque pour des règles d'ordre 25 les heuristiques issues des méthodes exactes s'expriment en termes de jours, voire d'années, alors que pour l'algorithme 2.1 les temps de calcul sont encore sous la barre des dixièmes de seconde.

TABLEAU 2.2 – Comparaison des résultats de l'algorithme 2.1

Nombre de marques	Algorithme 2.1	Méthode tabou	Longueur optimale
12	85	85	85
13	111	106	106
14	127	127	127
15	155	151	151
16	179	177	177
17	199	214	199
18	216	229	216
19	246	281	246
20	283	322	283
21	333	372	333
22	356	421	356
23	372	476	372
24	425	520	425
25	480	595	480

La première colonne du Tableau 2.2 représente le nombre de marques de la règle de Golomb voulue. Les trois autres colonnes sont, respectivement, la longueur obtenue par l'algorithme 2.1, la meilleure longueur obtenue par l'heuristique issue de la

méthode tabou de Galinier et Jaumard (2006), et, la longueur optimale de la règle de Golomb. En observant le Tableau 2.2, on peut voir que la solution optimale est obtenue dans tous les cas sauf trois, et dans ces trois cas, la solution est à moins de 5% de la solution optimale.

Pour montrer l'efficacité des méthodes algébriques et pour donner un aperçu de la variation des temps de calcul et de la longueur de règles de Golomb en fonction du nombre de marques, nous présentons dans le Tableau 2.3 les résultats obtenus par l'algorithme 2.1 pour les règles d'ordre supérieur à 25. La première colonne du tableau représente le nombre de marques, dans la seconde colonne on retrouve la longueur de la meilleure règle obtenue, et finalement, la dernière colonne nous donne le temps nécessaire, en secondes, pour obtenir la meilleure solution. Ces calculs ont été effectués sur un ordinateur muni d'un processeur de 3.40 GHz.

TABLEAU 2.3 – Résultats de l'algorithme 2.1 pour ordre supérieur à 25

Marques	Longueur	Temps (sec)	Marques	Longueur	Temps (sec)
25	480	< 1	400	153195	246
50	2094	1	425	173760	484
75	4982	2	450	194151	572
100	8831	5	475	216717	426
125	14055	22	500	240665	859
150	20521	14	525	266917	435
175	28293	19	550	292724	749
200	37356	9	575	320232	680
225	47166	75	600	348472	2250
250	58716	234	625	379320	2137
275	71421	145	650	409748	1602
300	85679	60	675	442470	3300
325	101013	73	700	476502	2201
350	116679	230	725	510251	5499
375	134859	327	750	548028	3600

2.4 Ensembles doublement orthogonaux

Dans cette section, nous proposons d'adapter les méthodes que nous avons utilisées pour construire les règles de Golomb afin de déterminer des ensembles doublement orthogonaux. Nous verrons que cette généralisation est possible à l'aide de quelques modifications seulement, et les propriétés généralisées seront également justifiées.

2.4.1 Généralités

Nous avons déjà vu deux manières distinctes de voir les points d'une géométrie projective construite sur un corps fini. Une autre façon, qui nous sera utile pour démontrer les propositions suivantes, est de considérer l'ensemble des polynômes modulo un polynôme primitif. Soit $f(x)$ un polynôme monique primitif de degré k dans $\mathbb{F}_q[x]$. Alors les trois corps $\mathbb{F}_q^k$, $\mathbb{F}_{q^k}$ et $\mathbb{F}_q[x]/(f)$ sont isomorphes. Autrement dit,

$$\mathbb{F}_q^k \cong \mathbb{F}_{q^k} \cong \mathbb{F}_q[x]/(f),$$

où (f) est l'idéal principal engendré par f. En effet, nous avons déjà vu une bijection entre $\mathbb{F}_q^k$ et $\mathbb{F}_{q^k}$. Une bijection entre $\mathbb{F}_q[x]/(f)$ et $\mathbb{F}_q^k$ est obtenue en considérant les polynômes de $\mathbb{F}_q[x]/(f)$ comme les vecteurs contenant leurs coefficients.

Si α est une racine de $f(x)$ alors les éléments de $\mathbb{F}_q[x]/(f)$ peuvent être vus comme les polynômes en α de degré inférieur ou égal à $k-1$. Si $g(\alpha) \in \mathbb{F}_q[x]/(f)$ et que $\deg(g) = d$ alors $g(\alpha)$ possède d racines, c'est-à-dire que $g(\alpha)$ s'écrit comme le produit de d facteurs linéaires, ou encore

$$g(\alpha) = (\alpha - \beta_1)(\alpha - \beta_2)\cdots(\alpha - \beta_d),$$

où $\beta_i \in \mathbb{F}_q$ pour $i = 1, 2, \ldots, d$.

Dans ce qui suit, nous utiliserons indifféremment, selon les besoins, les éléments de $\mathbb{F}_{q^k}$ (des puissances d'un élément primitif α) ou de $\mathbb{F}_q[x]/(f)$ (des polynômes), le contexte indiquant à quel type d'élément nous référons.

Exemple 2.69. *Pour illustrer ce qui vient d'être dit, reprenons le polynôme primitif,* $f(x) = x^3 + 2x^2 + x + 1 \in \mathbb{F}_3[x]$ *de l'exemple 2.52.*

Pour $f(x) = 0$, *nous obtenons alors la relation* $x^3 = x^2 + 2x + 2$, *nous permettant de voir les éléments de* $\mathbb{F}_3[x]/(f)$ *comme les puissances d'une racine* x *de* $f(x)$. *Ainsi, à chaque entier* $i \in \mathbb{F}_{3^3}^*$ *on associe bijectivement* i *au polynôme non nul correspondant à* x^{i-1} *dans* $\mathbb{F}_3[x]/(f)$, *puis à ce polynôme on associe le triplet de* $\mathbb{F}_3^3$ *correspondant aux coefficients du polynôme. Le Tableau 2.4 indique les correspondances entre les éléments des trois ensembles pour les bijections proposées.*

2.4.2 $PG(4, \mathbb{F}_q)$ et ensembles doublement orthogonaux

Dans ce qui suit nous considérons la partition des $(m+1)$-tuples d'éléments de $\mathbb{F}_q$ qui associe deux $(m+1)$-tuples à une même classe si et seulement si l'un est le produit de l'autre par un scalaire de $\mathbb{F}_q$. En prenant les représentants de classe de cette partition pour points de $PG(m, \mathbb{F}_q)$, un k-espace, pour $1 \leq k < m$, s'exprime alors comme l'ensemble des points p satisfaisant $D * p = 0$, où D est une matrice de plein rang d'ordre $(m-k) \times (m+1)$. En particulier, dans $PG(4, \mathbb{F}_q)$, une droite D est formée des points p qui sont des 5-tuples non nuls de $\mathbb{F}_q^5$ et qui satisfont $D * p = 0$, où D est une matrice d'ordre 3×5 de rang 3 sur le corps $\mathbb{F}_q$.

Étant donné deux points p_1 et p_2 appartenant à une droite D, toutes les combinaisons linéaires de p_1 et p_2 forment la droite D. En effet, puisque

$$Dp_i = 0 \Rightarrow D(\alpha p_i) = 0, \ \forall \alpha \in \mathbb{F}_q \text{ et } i = 1, 2,$$

alors

$$D(\alpha p_1 + \beta p_2) = D(\alpha p_1) + D(\beta p_2) = 0, \ \forall \alpha, \beta \in \mathbb{F}_q.$$

TABLEAU 2.4 – Correspondances entre les différents types d'éléments d'un corps fini.

$\mathbb{F}_{3^3}$	$\mathbb{F}_3[x]/(x^3+2x^2+x+1)$	$\mathbb{F}_3^3$
0	0	(0,0,0)
1	$x^0 = 1$	(0,0,1)
2	$x^1 = x$	(0,1,0)
3	$x^2 = x^2$	(1,0,0)
4	$x^3 = x^2 + 2x + 2$	(1,2,2)
5	$x^4 = x + 2$	(0,1,2)
6	$x^5 = x^2 + 2x$	(1,2,0)
7	$x^6 = 2x + 2$	(0,2,2)
8	$x^7 = 2x^2 + 2x$	(2,2,0)
9	$x^8 = x^2 + x + 1$	(1,1,1)
10	$x^9 = 2x^2 + 2$	(2,0,2)
11	$x^{10} = 2x^2 + 1$	(2,0,1)
12	$x^{11} = 2x^2 + 2x + 1$	(2,2,1)
13	$x^{12} = x^2 + 2x + 1$	(1,2,1)
14	$x^{13} = 2$	(0,0,2)
15	$x^{14} = 2x$	(0,2,0)
16	$x^{15} = 2x^2$	(2,0,0)
17	$x^{16} = 2x^2 + x + 1$	(2,1,1)
18	$x^{17} = 2x + 1$	(0,2,1)
19	$x^{18} = 2x^2 + x$	(2,1,0)
20	$x^{19} = x + 1$	(0,1,1)
21	$x^{20} = x^2 + x$	(1,1,0)
22	$x^{21} = 2x^2 + 2x + 2$	(2,2,2)
23	$x^{22} = x^2 + 1$	(1,0,1)
24	$x^{23} = x^2 + 2$	(1,0,2)
25	$x^{24} = x^2 + x + 2$	(1,1,2)
26	$x^{25} = 2x^2 + x + 2$	(2,1,2)

Le fait qu'étant donné deux points appartenant à une droite, tous les autres points de la droite sont les combinaisons linéaires de ces deux points est illustré dans l'exemple suivant.

Exemple 2.70. *Soit*

$$D = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

une droite de $PG(4, \mathbb{F}_3)$. *En prenant pour convention que les représentants de classe des* 5*-tuples d'éléments de* $\mathbb{F}_3$ *sont les* 5*-tuples dont le premier élément non nul est* 1, *on trouve aisément que les points* $(0,0,0,0,1)$ *et* $(0,0,0,1,0)$ *appartiennent à cette droite. Les combinaisons linéaires de ces deux points satisfaisant nos conventions sont alors* $(0,0,0,1,1)$ *et* $(0,0,0,1,2)$. *Il est aisé de vérifier que ces deux points appartiennent à la droite et nous pouvons également vérifier qu'aucun autre point ne peut appartenir à cette droite.*

Ainsi, la droite D est bien constituée des quatres points suivants :

$$(0,0,0,0,1),$$
$$(0,0,0,1,0),$$
$$(0,0,0,1,1), \text{ et}$$
$$(0,0,0,1,2),$$

et chaque point peut être exprimé comme une combinaison linéaire de deux autres points.

La prochaine notion est une généralisation des règles de Golomb appelée ensemble doublement orthogonal. De même que pour les règles de Golomb usuelles, les entiers formant ces ensembles sont appelés les marques et les mêmes conventions que pour les règles de Golomb sont observées pour les indices des marques. Pour ces ensembles, en plus de demander que les différences pour chaque paire de marques soient distinctes, on demande que les différences entre les différences générées soient distinctes sous certaines conditions. Il est important de noter qu'il n'est pas possible de construire des ensembles d'entiers tels que toutes les différences et différences de différences soient distinctes. Par exemple, il est évident qu'étant donné les différences $|g_i - g_j|$ et $|g_k - g_j|$ la différence entre ces deux différences peut être égale à $|g_i - g_k|$ qui est une différence de la règle. Ce problème est évité en définissant les ensembles doublement

orthogonaux avec certaines conditions sur les indices des marques comme il est fait dans la définition suivante.

Définition 2.71. *Un ensemble d'entiers* $E = \{g_i\}_{i \geq 0}$ *est dit* doublement orthogonal au sens large *si pour tous les* 4*-tuples d'indices* (i, j, k, ℓ) *satisfaisant*

$$k \neq \ell, j \neq k, i \geq k, j \geq \ell \text{ et } i > j,$$

les valeurs $|g_i - g_j|$ *et* $|(g_i - g_j) - (g_\ell - g_k)|$ *sont toutes distinctes.*

Exemple 2.72. *L'ensemble* $E = \{0, 1, 11, 15\}$ *est doublement orthogonal. Pour s'en convaincre, il suffit de vérifier pour tous les 4-tuples d'indices satisfaisant les conditions indiquées à la définition 2.71 que toutes les différences générées sont distinctes. La liste des différences engendrées est la suivante :*

$$
\begin{aligned}
&(1,0) \Rightarrow |1-0| = 1\\
&(2,0) \Rightarrow |11-0| = 11\\
&(2,1) \Rightarrow |11-1| = 10\\
&(3,0) \Rightarrow |15-0| = 15\\
&(3,1) \Rightarrow |15-1| = 14\\
&(3,2) \Rightarrow |15-11| = 4\\
&(1,0,1,0) \Rightarrow |(1-0)-(0-1)| = 2\\
&(2,0,1,0) \Rightarrow |(11-0)-(0-1)| = 12\\
&(2,0,2,0) \Rightarrow |(11-0)-(0-11)| = 22\\
&(2,1,0,1) \Rightarrow |(11-1)-(1-0)| = 9\\
&(2,1,2,0) \Rightarrow |(11-1)-(0-11)| = 21\\
&(2,1,2,1) \Rightarrow |(11-1)-(1-11)| = 20\\
&(3,0,1,0) \Rightarrow |(15-0)-(0-1)| = 16\\
&(3,0,2,0) \Rightarrow |(15-0)-(0-11)| = 26\\
&(3,0,3,0) \Rightarrow |(15-0)-(0-15)| = 30\\
&(3,1,0,1) \Rightarrow |(15-1)-(1-0)| = 13\\
&(3,1,2,0) \Rightarrow |(15-1)-(0-11)| = 25\\
&(3,1,2,1) \Rightarrow |(15-1)-(1-11)| = 24\\
&(3,1,3,0) \Rightarrow |(15-1)-(0-15)| = 29\\
&(3,1,3,1) \Rightarrow |(15-1)-(1-15)| = 28\\
&(3,2,0,1) \Rightarrow |(15-11)-(1-0)| = 3\\
&(3,2,0,2) \Rightarrow |(15-11)-(11-0)| = 7\\
&(3,2,1,0) \Rightarrow |(15-11)-(0-1)| = 5\\
&(3,2,1,2) \Rightarrow |(15-11)-(11-1)| = 6\\
&(3,2,3,0) \Rightarrow |(15-11)-(0-15)| = 19\\
&(3,2,3,1) \Rightarrow |(15-11)-(1-15)| = 18\\
&(3,2,3,2) \Rightarrow |(15-11)-(11-15)| = 8
\end{aligned}
$$

Puisque toutes les différences considérées sont distinctes alors l'ensemble E est bien doublement orthogonal.

L'utilité des ensembles doublement orthogonaux se situe au niveau des codes correcteurs d'erreurs. Comme pour les règles de Golomb usuelles, ces ensembles génèrent directement des codes appelés codes convolutionnels doublement orthogonaux (CSO^2C, Convolutionnal Self Doubly Orthogonal Codes). Pour plus de détails concernant ce type de codes le lecteur peut consulter l'article de Cardinal, Haccoun, Gagnon et Batani (1999), où ces codes ont été présentés.

Nous voulons maintenant montrer comment obtenir un ensemble doublement orthogonal à partir de la construction d'une géométrie projective de dimension 4. Le lemme suivant, qui est une condition suffisante pour qu'un ensemble soit doublement orthogonal, nous sera utile pour démontrer que les ensembles considérés sont bien doublement orthogonaux.

Lemme 2.73. *Étant donné un ensemble d'entiers $E = \{g_i\}_{i\geq 0}$, si pour toutes paires de multi-ensembles distincts de quatre indices, $\{i,j,k,\ell\} \neq \{i',j',k',\ell'\}$, on a*

$$g_i + g_j + g_k + g_\ell \neq g_{i'} + g_{j'} + g_{k'} + g_{\ell'}$$

alors l'ensemble E est doublement orthogonal.

Preuve. Supposons qu'il existe $(i,j,k,\ell) \neq (i',j',k',\ell')$ satisfaisant

$$\begin{gathered} i > j, k \neq \ell, j \neq k, i \geq k, j \geq \ell \text{ et} \\ i' > j', k' \neq \ell', j' \neq k', i' \geq k', j' \geq \ell', \end{gathered}$$

tels que $(g_i - g_j) - (g_\ell - g_k) = (g_{i'} - g_{j'}) - (g_{\ell'} - g_{k'})$.

Ceci implique que $g_i + g_{j'} + g_k + g_{\ell'} = g_{i'} + g_j + g_{k'} + g_\ell$, et par conséquent, que $\{i,j',k,\ell'\} = \{i',j,k',\ell\}$, puisque toutes les sommes sont distinctes. Autrement dit, $(i,j',k,\ell') = \sigma(i',j,k',\ell)$, où σ est une permutation dans $\mathbb{S}_4$.

Or, on a par hypothèse $i \neq \ell$, $j \neq k$, $i \neq j$ et $\ell \neq k$, il faut donc que $\sigma(i) = i'$ ou k', et que $\sigma(k) = i'$ ou k'. Considérons ces quatre cas.

1. Cas $(i,j',k,\ell') = (i',j,k',\ell)$. Ceci implique que $(i,j,k,\ell) = (i',j',k',\ell')$ contredisant l'hypothèse de départ ;
2. Cas $(i,j',k,\ell') = (i',\ell,k',j)$. Puisque $\ell \leq j$ et que $\ell' \leq j'$ alors on a

   $$\ell' = j \geq \ell = j' \geq \ell'$$

   et ainsi $\ell = j = \ell' = j'$. Ce qui est équivalent au cas précédent ;

3. Cas $(i, j', k, \ell') = (k', \ell, i', j)$. On a

$$i = k' \leq i' = k \leq i \text{ et } \ell' = j \geq \ell = j' \geq \ell'$$

ce qui implique $i = k = i' = k'$ et $\ell = j = \ell' = j'$, contredisant encore l'hypothèse $(i, j, k, \ell) \neq (i', j', k', \ell')$;

4. Cas $(i, j', k, \ell') = (k', j, i', \ell)$. Puisque $\ell \leq j$ et que $\ell' \leq j'$ alors $\ell = j = \ell' = j'$. Ce qui est équivalent au cas précédent.

Tous les cas possibles mènent à une contradiction, la supposition que nous avons faite est donc fausse.

De plus, si une différence simple est égale à une autre différence simple ou à une différennce double alors il existe nécessairement $\{i, j, k, \ell\} \neq \{i', j', k', \ell'\}$, deux multi-ensembles distincts de quatre indices, tels que $g_i + g_j + g_k + g_\ell \neq g_{i'} + g_{j'} + g_{k'} + g_{\ell'}$ puisqu'il est alors possible de compléter les ensembles d'indices avec l'indice d'un même élément. Ainsi, le cas des différences simples est vérifié et le résultat voulu est démontré.

□

Nous voulons maintenant démontrer que chacune des droites d'une géométrie projective forme un ensemble doublement orthogonal. En utilisant le lemme 2.73, il suffit de montrer que chacune des droites forme un ensemble dont toutes les sommes sont distinctes. Pour ce faire considérons la structure de $\mathbb{F}_{q^5}$. Comme nous l'avons déjà mentionné, $\mathbb{F}_{q^5}$ peut être vu comme l'ensemble des q^5 polynômes de degré inférieur ou égal à quatre sur $\mathbb{F}_q$. Si on prend α pour racine de $f(x)$, un polynôme primitif, alors le groupe multiplicatif $\mathbb{F}_{q^5}^*$ est engendré par α. Une bijection φ des puissances de α sur les polynômes non nuls de degré inférieur ou égal à quatre est donnée par :

$$\varphi : \alpha^n \mapsto \alpha^n \mod f(\alpha).$$

Pour obtenir un ensemble dont toutes les sommes sont distinctes il suffit alors de prendre l'ensemble des puissances correspondant par φ^{-1} aux polynômes sur une droite de la géométrie projective.

En effet, puisque la décomposition en facteurs premiers de tous les polynômes moniques de degré inférieur ou égal à quatre est unique et que pour tout polynôme f il existe un entier n tel que $f(\alpha) = \alpha^n$, alors en notant $\alpha^{g_i} = \varphi^{-1}(\alpha + i)$, avec $i \in \mathbb{F}_q$ on obtient :

$$\begin{aligned}
&\{i, j, k, \ell\} \neq \{i', j', k', \ell'\} \\
\Leftrightarrow\ &(\alpha + i)(\alpha + j)(\alpha + k)(\alpha + \ell) \neq (\alpha + i')(\alpha + j')(\alpha + k')(\alpha + \ell') \\
\Leftrightarrow\ &\alpha^{g_i}\alpha^{g_j}\alpha^{g_k}\alpha^{g_\ell} \neq \alpha^{g_{i'}}\alpha^{g_{j'}}\alpha^{g_{k'}}\alpha^{g_{\ell'}} \\
\Leftrightarrow\ &\alpha^{g_i+g_j+g_k+g_\ell} \neq \alpha^{g_{i'}+g_{j'}+g_{k'}+g_{\ell'}} \\
\Leftrightarrow\ &g_i + g_j + g_k + g_\ell \neq g_{i'} + g_{j'} + g_{k'} + g_{\ell'}.
\end{aligned}$$

Notons que dans le cas des polynômes de degré inférieur à quatre, cela revient à dire qu'un ou plusieurs facteurs sont remplacés par des polynômes constants.

Ainsi, nous venons de démontrer que les entiers $\{g_i \mid 0 \leq i \leq q\}$ constituant une droite dans $PG(4, q)$ satisfont la condition des sommes distinctes. En combinant ce résultat au lemme 2.73, on obtient directement le théorème qui suit.

Théorème 2.74. *Soit $\{g_i \mid 0 \leq i \leq q\}$ un ensemble d'entiers constituant une droite dans $PG(4, q)$. Alors $\{g_i \mid 0 \leq i \leq q\}$ est un ensemble doublement orthogonal.*

Étant donné $\{g_i \mid 0 \leq i \leq q\}$ un ensemble d'entiers constituant une droite dans $PG(4, q)$, il est possible d'appliquer certaines opérations sur cet ensemble pour obtenir d'autres ensembles doublement orthogonaux. Ces opérations appelées *décalage* et *multiplicateur*, sont présentées dans la suite de cette section.

Remarque 2.75. *Pour ce qui suit, il est important de se rappeler que les points de $PG(4,q)$ peuvent indifféremment être vus, selon les différentes bijections données, comme des entiers, des polynômes de degré au plus quatre ou encore des 5-tuples d'éléments de $\mathbb{F}_q$. Pour démontrer les résultats qui suivent, nous adoptons la notation polynomiale, en rappelant qu'un polynôme de degré 4 en α peut être vu comme une puissance de α.*

La remarque 2.75 nous permet de définir les opérations de décalage et les multiplicateurs sur des droites considérées comme des ensembles de puissances de α. Le résultat pour les ensembles d'entiers est alors simplement obtenu en considérant la bijection qui associe à α^n l'entier n.

Définition 2.76. *Étant donné une droite $D = \{\alpha^{g_0}, \alpha^{g_1}, ..., \alpha^{g_q}\}$ on dit que l'ensemble $D' = \{\alpha^{g_0+k}, \alpha^{g_1+k}, ..., \alpha^{g_q+k}\}$, où les entiers $g_i + k$ sont pris modulo $\frac{q^5-1}{q-1}$, est un* décalage de longueur k *de D.*

Remarque 2.77. *Pour la construction de la géométrie projective de dimension 4, nous identifions les polynômes qui sont multiples d'un scalaire. Autrement dit, si $\beta \in \mathbb{F}_{q^5}$ est pris pour représenter sa classe d'équivalence, alors nous identifions $i\beta$ à β pour tout $i \in \mathbb{F}_q^*$. De plus, on aura*

$$\beta = \{i\beta \mid \beta \in \mathbb{F}_{q^5}, i \in \mathbb{F}_q^*\} = \{\alpha^{i\left(\frac{q^5-1}{q-1}\right)}\beta \mid i \in \mathbb{F}_q^*\}.$$

En utilisant cette remarque et la définition d'un décalage, nous sommes en mesure de démontrer la proposition suivante.

Proposition 2.78. *Soit D une droite dans une géométrie projective de dimension 4. Alors tous les ensembles obtenus de D par un décalage sont également des droites d'une géométrie projective de dimension 4.*

Preuve. En effet, soient $D = \{\alpha^{g_0}, \alpha^{g_1}, ..., \alpha^{g_q}\}$ une droite de $PG(4,q)$ et $E = \{\alpha^{g_0+k}, \alpha^{g_1+k}, ..., \alpha^{g_q+k}\}$ l'ensemble des polynômes obtenus en multipliant les éléments

de D par α^k. On sait que tous les élements de E sont des points de $PG(4,q)$ et on sait qu'une droite de $PG(4,q)$ peut être vue comme les combinaisons linéaires de n'importe quelle paire de point qui la compose. Prenons $\alpha^{g_0+k}, \alpha^{g_1+k} \in E$ et regardons les combinaisons linéaires de ces deux points. Pour n'importe quels scalaires $\beta, \gamma \in \mathbb{F}_q$, on a

$$\beta\alpha^{g_0+k} + \gamma\alpha^{g_1+k} = (\beta\alpha^{g_0} + \gamma\alpha^{g_1})\alpha^k.$$

Or, $\beta\alpha^{g_0} + \gamma\alpha^{g_1}$ est une combinaison linéaire d'éléments de D, par conséquent, il existe donc un entier $i \neq 0, 1$ tel que $\beta\alpha^{g_0} + \gamma\alpha^{g_1} = \alpha^{g_i}$. Ainsi, l'élément $\alpha^{g_i+k} \in E$ est bien obtenu par une combinaison linéaire d'élément de E puisqu'on a

$$\beta\alpha^{g_0+k} + \gamma\alpha^{g_1+k} = (\beta\alpha^{g_0} + \gamma\alpha^{g_1})\alpha^k = \alpha^{g_i+k}.$$

Puisque le même raisonnement s'applique pour toutes les valeurs des scalaires $\beta, \gamma \in \mathbb{F}_q$ alors le résultat est démontré, c'est-à-dire, E est bien une droite d'une géométrie projective de dimension 4. □

Définition 2.79. *Étant donné une droite $D = \{\alpha^{g_0}, \alpha^{g_1}, ..., \alpha^{g_q}\}$ et un entier k tel que $(k, q^5 - 1) = 1$, on dit que k est un* multiplicateur *de D et l'ensemble associé à ce multiplicateur est $D' = \{\alpha^{kg_0}, \alpha^{kg_1}, ..., \alpha^{kg_q}\}$, où les puissances de α sont prises modulo $\frac{q^5-1}{q-1}$.*

Proposition 2.80. *Soit D une droite dans une géométrie projective de dimension 4. Alors tous les ensembles obtenus de D par un multiplicateur sont également des droites d'une géométrie projective de dimension 4.*

Preuve. Soient $D = \{\alpha^{g_0}, \alpha^{g_1}, ..., \alpha^{g_q}\}$ une droite dans $\mathcal{G}$, une géométrie projective de dimension 4 et m un multiplicateur de D. Les points de $\mathcal{G}$ sont alors vus comme des puissances de α, c'est-à-dire comme des éléments de $\{\alpha^i \mid 0 \leq i \leq \frac{q^5-1}{q-1}\}$. Puisque par définition, m est relativement premier à $\frac{q^5-1}{q-1}$, on sait que la fonction

$$\phi_m(i) = m * i \mod \frac{q^5 - 1}{q - 1}$$

est une bijection sur les entiers modulo $\frac{q^5-1}{q-1}$. Par conséquent, la fonction

$$\Phi(\alpha^i) = \alpha^{\phi_m(i)}$$

est également une bijection entre les points de la géométrie $\mathcal{G}$. Puisque Φ est une bijection sur les points de $\mathcal{G}$ alors n'importe quel ensembles de points correspondant à une droite est envoyé sur un unique ensemble de points et les relations entre les droites de $\mathcal{G}$ demeurent les mêmes après l'application de Φ. Il en est également de même pour n'importe quel μ-espace de $\mathcal{G}$ et par conséquent, Φ induit un automorphisme (isomorphisme d'une structure sur elle-même) sur $\mathcal{G}$. Autrement dit, si on note $\mathcal{G}'$ la structure obtenue en définissant récursivement (en partant des points, c'est-à-dire les 0-espaces) les μ-espaces de $\mathcal{G}'$ comme l'image des μ-espaces de $\mathcal{G}$ par Φ alors $\mathcal{G}'$ est isomorphe à $\mathcal{G}$. Ainsi à toute droite de $\mathcal{G}$ correspond, par Φ, une droite de $\mathcal{G}'$.

En appliquant le multiplicateur m sur la droite de départ D, on obtient l'ensemble $D' = \{\alpha^{mg_0}, \alpha^{mg_1}, ..., \alpha^{mg_q}\}$ qui, par définition de Φ, est une droite de la géométrie $\mathcal{G}'$. Puisque le multiplicateur m et la droite D étaient quelconque alors le résultat est vérifié pour tous les multiplicateurs et toutes les droites.

□

Étant donné une droite d'une géométrie projective de dimension 4, il est possible, grâce à la proposition 2.78 et à la proposition 2.80, de générer une multitude de nouvelles droites et donc de nouveaux ensembles doublement orthogonaux. Cette propriété est, comme pour les règles de Golomb usuelles, le point central de notre méthode de construction des ensembles doublement orthogonaux.

2.4.3 Algorithme pour les ensembles doublement orthogonaux

Suite aux résultats précédents, nous sommes maintenant en mesure de formuler un algorithme pour déterminer des ensembles doublement orthogonaux. En effet,

avec quelques modifications mineures, l'algorithme présenté pour les règles de Golomb se généralise pour le cas des ensembles doublement orthogonaux. Dans le cas présent, nous construisons des CDS doublement orthogonaux, c'est-à-dire des ensembles doublement orthogonaux muni d'un module (voir ci-après la définition 2.85). Le pseudo-code est présenté dans l'algorithme 2.2.

Algorithme 2.2 Construction des droites de $PG(4, q)$

Antécédent: q une puissance de nombre premier et L la liste des polynômes de degré 5 sur $\mathbb{F}_q$;
Conséquent: $\mathcal{E}$ un ensemble de droites projectives de $PG(4, q)$

1: $\mathcal{E} = \emptyset$
2: **pour tout** $f \in L$ **faire**
3: **si** f est primitif **alors**
4: Construire la suite $S(f)$
5: Trouver une droite D contenant le point (0,0,0,0,1)
6: Convertir D en ensemble d'entiers E avec la fonction $POS_{S(f)}$
7: **pour** $i = 0$ **à** $\frac{q^5-1}{q-1} - 1$ **faire**
8: Appliquer tous les multiplicateurs sur E avec décalage de i
9: Ajouter à $\mathcal{E}$ les droites n'y apparaissant pas déjà
10: **fin pour**
11: **fin si**
12: **fin pour**
13: **retourner** l'ensemble $\mathcal{E}$

Comme dans le cas des règles de Golomb usuelles, la construction d'ensembles doublement orthogonaux pour un nombre de marques qui est éloigné d'une puissance d'un nombre premier, s'obtient en enlevant des marques. Les longueurs des meilleurs ensembles doublement orthogonaux obtenus de cette manière sont présentées dans le Tableau 2.5 dans la section 2.4.5.

Une étude de la structure des géométries projectives nous donne une première borne supérieure sur la longueur des ensembles doublement orthogonaux. En effet, sachant que le nombre de points dans $PG(4, q)$ est $\frac{q^5-1}{q-1}$, ce nombre induit une borne supérieure triviale sur la longueur des ensembles doublement orthogonaux. Autrement

dit, en notant $\Delta\Delta(J)$ la longueur minimale d'un ensemble doublement ortogonal d'ordre J, nous avons le résultat suivant :

Proposition 2.81. *Soit q la plus petite puissance d'un entier naturel supérieure ou égal à $J-1$. On a*

$$\Delta\Delta(J) < \frac{q^5-1}{q-1}.$$

En remarquant qu'entre les entiers J et $2J-1$ il existe toujours une puissance d'un nombre premier, en l'occurence une puissance de 2, on peut reprendre le résultat précédent et obtenir la borne supérieure suivante.

Proposition 2.82. *Soit J l'ordre d'un ensemble doublement orthogonal. On a*

$$\Delta\Delta(J) < \frac{(2J-1)^5-1}{(2J-1)-1} = 16J^4 - 88J^3 + 184J^2 - 172J + 61.$$

La définition 2.71 permet de déterminer une borne inférieure sur la longueur d'un ensemble doublement orthogonal. En effet, le dénombrement des contraintes exigeant que les différences de différences et les différences soient distinctes nous donne une borne inférieure sur la longueur d'un ensemble doublement orthogonal. On peut calculer N_c le nombre des contraintes considérées, et obtenir :

$$N_c = \frac{J^4 - 2J^3 + 7J^2 - 6J}{16}.$$

On obtient alors la borne inférieure triviale sur $\Delta\Delta(J)$ énoncée dans la proposition suivante.

Proposition 2.83. *(Haccoun et al., 2005) Soit J l'ordre d'un ensemble doublement orthogonal. On a*

$$\Delta\Delta(J) > \frac{J^4 - 2J^3 + 7J^2 - 6J}{16}.$$

La proposition 2.82 combinée à la proposition 2.83 nous donne alors un ordre de grandeur pour la valeur de $\Delta\Delta(J)$. Ceci est exprimé sous forme de résultat dans le corollaire suivant.

Corollaire 2.84. *Soit J l'ordre d'un ensemble doublement orthogonal. On a*

$$\Delta\Delta(J) = \Theta(J^4).$$

Bien que les droites d'une géometrie projective nous donnent une borne supérieure intéressante (dans l'ordre de J^4) sur la longueur des ensembles doublement orthogonaux, il demeure possible d'améliorer ces dernières en appliquant des opérations arithmétiques valides sur les ensembles fournis. En particulier, pour les ensembles ayant un petit ordre il est possible d'appliquer, avec des temps de calcul relativement peu coûteux, des opérations pour obtenir de nouveaux ensembles doublement orthogonaux. Dans la prochaine section nous présentons une heuristique de réduction basée sur ces opérations.

2.4.4 Réductions

Nous avons vu que n'importe quelle droite issue d'une géometrie projective de dimension 4 forme un ensemble doublement orthogonal. Puisqu'il existe une infinité de géométries projectives de dimension 4 nous en concluons qu'il est possible d'obtenir autant d'ensembles doublement orthogonaux que nous désirons. Toutefois, à l'exception du module induit par l'ordre de la géométrie, nous n'avons aucun contrôle sur la longueur des ensembles ainsi générés. Pour réduire la longueur d'un ensemble doublement orthogonal nous utiliserons les opérations de décalage et les multiplicateurs déjà utilisés pour générer les droites projectives. Pour utiliser ces opérations il faut alors définir un module valide pour un ensemble doublement orthogonal. Ceci est l'objet de la définition suivante.

Définition 2.85. *Soit $E = \{g_0, g_1, g_2, \ldots, g_J\}$ un ensemble doublement orthogonal. Un entier n est un* module valide *pour E si pour tous les 4-tuples d'indices (i, j, k, ℓ) satisfaisant*

$$k \neq \ell, j \neq k, i \neq \ell, i \geq k, j \geq \ell \text{ et } i \neq j,$$

les valeurs $g_i - g_j$ et $(g_i - g_j) - (g_\ell - g_k)$ sont toutes distinctes modulo n.

Remarque 2.86. *Nous avons déjà vu le lien qui existe entre les règles de Golomb et les CDS, la même relation existe entre les ensembles doublement orthogonaux et les ensembles doublement orthogonaux modulo n. Dans un cas les différences négatives sont permises alors que dans l'autre cas les différences sont considérées modulo n, et par conséquent elles sont toutes positives. Cette observation nous conduit, étant donné un ensemble doublement orthogonal E, à une première valeur possible comme module valide pour E. En effet, si g_J est la longueur de E alors toutes les différences et différences de différences se trouvent dans l'intervalle allant de $-2g_J$ à $2g_J$. Ainsi, en prenant $n = 4g_J+1$ pour module de E on est alors assuré que toutes les différences modulo n soient distinctes.*

Comme nous venons de le dire, étant donné un ensemble doublement orthogonal de longueur g_J, un module valide pour cet ensemble est donné par $4g_J + 1$. Remarquons que de la même façon, n'importe quel entier supérieur à $4g_J + 1$ est également un module valide pour cet ensemble. Ainsi, il existe donc une infinité de modules valides pour un ensemble doublement orthogonal donné. La procédure de réduction de la longueur des ensembles doublement orthogonaux que nous proposons est intimement liée à la notion de module valide. L'idée de cette méthode consiste simplement à appliquer les opérations de décalages et les multiplicateurs, comme nous l'avons déjà fait pour les droites projectives, en faisant varier le module de l'ensemble doublement orthogonal. La justification de ces opérations est donnée par la proposition suivante.

Proposition 2.87. *(Haccoun et al., 2005) Soit $E = \{g_0, g_1, g_2, \ldots, g_J\}$ un ensemble doublement orthogonal et n un module valide pour E. Alors pour tout entier d, $1 \leq d < n$ et pour tout entier m relativement premier à n, on a que*

$$E' = \{mg_0 + d, mg_1 + d, mg_2 + d, \ldots, mg_J + d\} \mod n$$

est aussi un ensemble doublement orthogonal.

Preuve. En effet, puisque $E = \{g_0, g_1, g_2, \ldots, g_J\}$ est un ensemble doublement orthogonal et que n est un module valide, on a

$$((g_i - g_j) - (g_\ell - g_k)) \mod n \neq ((g_{i'} - g_{j'}) - (g_{\ell'} - g_{k'})) \mod n$$

pour toutes paires de 4-tuples d'indices (i, j, k, ℓ) et (i', j', k', ℓ') satisfaisants les conditions de la définition 2.85.

Comme m est relativement premier à n alors pour tout entiers a et b on a

$$a \neq b \mod n \Rightarrow ma \neq mb \mod n.$$

Donc en particulier, on a

$$(m((g_i - g_j) - (g_\ell - g_k))) \mod n \neq (m((g_{i'} - g_{j'}) - (g_{\ell'} - g_{k'}))) \mod n$$

qui est équivalent à

$$((mg_i - mg_j) - (mg_\ell - mg_k)) \mod n \neq ((mg_{i'} - mg_{j'}) - (mg_{\ell'} - mg_{k'})) \mod n.$$

On a également

$$((mg_i + d - mg_j + d) - (mg_\ell + d - mg_k + d)) \mod n \neq$$

$$((mg_{i'} + d - mg_{j'} + d) - (mg_{\ell'} + d - mg_{k'} + d)) \mod n$$

puisque de part et d'autre de l'équation on ajoute la même valeur, en l'occurence 0.

Comme cela est vrai pour n'importe quelle paire de 4-tuples d'indices (i, j, k, ℓ) et (i', j', k', ℓ') satisfaisants les conditions de la définition 2.85, l'ensemble E' est doublement orthogonal et la proposition est démontrée.

□

Nous sommes maintenant en mesure d'énoncer la procédure de réduction. Mentionnons tout d'abord que l'idée de réduire les ensembles doublement orthogonaux avec les opérations mentionnés ci-dessus a déjà été utilisé par Haccoun (2005). Notre procédure diffère de celle de Haccoun principalement par le choix du module valide,

contrairement à Haccoun, nous recherchons d'abord avec les plus petits modules valides, ce qui semble, de manière empirique, être plus efficace pour trouver de meilleurs ensembles. Nous présentons maintenant les démarches de cette procédure.

Étant donné un ensemble doublement orthogonal E, nous utilisons tout d'abord une procédure itérative pour déterminer le plus petit module valide pour E. Cette procédure vérifie successivement tous les entiers jusqu'à l'obtention d'un module valide. Il est important de noter que la vérification de la double orthogonalité d'un ensemble d'ordre J se fait en temps $\mathcal{O}(J^4)$ et comme les valeurs de J que nous considérons sont relativement petites, cette vérification s'effectue très rapidement. En effet, puisque la recherche d'un module valide pour l'ensemble E consiste simplement à vérifier si l'ensemble est doublement orthogonal pour ce module, le temps de recherche de ce dernier dépend directement du temps de vérification des contraintes de double orthogonalité.

Après l'obtention d'un module valide n, nous appliquons les opérations de décalages ainsi que tous les multiplicateurs possibles sur l'ensemble E modulo n. Suite à l'application de ces opérations, deux choix se présentent : soit tous les ensembles considérés sont de longueur supérieure ou égale à la longueur de E ou soit nous avons trouvé un nouvel ensemble E' dont la longueur est inférieure à la longueur de E. Pour éviter de boucler à l'infini sans amélioration, un compteur doit être ajouté pour déterminer le nombre d'itérations sans qu'il y ait eu de diminution de la longueur de l'ensemble. Dans le cas où nous obtenons un ensemble E' de longueur inférieure à la longueur de l'ensemble E alors le compteur est réinitialisé à 0 et on réitère la procédure de réduction, depuis le début, avec l'ensemble E'. Si, au contraire, nous n'obtenons pas une longueur inférieure à l'ensemble de départ alors le compteur est incrémenté de un et nous cherchons le prochain module valide. Le compteur peut être incrémenté jusqu'à une valeur déterminée au préalable avant d'interrompre le processus, c'est-à-dire d'obtenir une condition d'arrêt. Cette valeur maximale du compteur doit être déterminée empiriquement avec pour unique but la terminaison de l'heuristique.

On peut résumer la procédure de réduction que nous suggérons par le pseudo-code (algorithme 2.3) suivant.

Algorithme 2.3 Réduction de la longueur des ensembles doublement orthogonaux

Antécédent: une liste L d'ensembles doublements orthogonaux d'ordre J et C_{max} le nombre d'itérations permis sans diminution de longueur ;
Conséquent: l'ensemble doublement orthogonal d'ordre J de longueur minimale pour les paramètres fixés

1: **pour tout** $E \in L$ **faire**
2: Initialiser le compteur C et le module n à 0
3: **tant que** $C \leq C_{max}$ **faire**
4: Affecter à n la valeur du prochain module valide pour E
5: Appliquer les opérations de décalages et les multiplicateurs modulo n
6: Retourner E' l'ensemble de longueur minimale
7: **si** $longueur(E') < longueur(E)$ **alors**
8: $C = 0$, $n = 0$ et $E = E'$
9: **sinon**
10: $C = C + 1$ et $n = n + 1$
11: **fin si**
12: **fin tant que**
13: **fin pour**
14: **retourner** l'ensemble avec la plus petite longueur

2.4.5 Résultats

Les longueurs des meilleurs ensembles doublement orthogonaux obtenus par les méthodes algébriques sont présentées dans le Tableau 2.5. La première colonne de ce tableau indique le nombre de marques des ensembles doublement orthogonaux en considérant que la première marque est 0. La colonne intitulée *géométrique* donne la longueur des meilleurs ensembles obtenus par les géométries semies-affines et projectives, les longueurs obtenues par les géométries semies-affines sont indiquées par le symbole a mis en exposant. La dernière colonne intitulée *Haccoun* contient les longueurs des meilleurs ensembles connus avant notre études, ils correspondent aux

longueurs des ensembles doublement orthogonaux obtenus par une méthode de génération pseudo-aléatoire conçue par Haccoun et al. (2005).

Pour analyser les résultats du Tableau 2.5, il est important de se rappeler que notre méthode de recherche d'ensembles doublement orthogonaux est une heuristique, c'est-à-dire que notre recherche ne peut pas être considérée comme une recherche exhaustive. En effet, comme nous l'avons déjà dit, il existe une infinité de géométries projectives et donc de droites correspondant à des ensembles doublement orthogonaux. Étant donné un ensemble doublement orthogonal on peut, selon le cas, démontrer que cet ensemble ne correspond à aucune droite de $PG(4, q)$, pour un q fixé. Toutefois, puisque tout sous-ensemble d'un ensemble doublement orthogonal est lui-même doublement orthogonal il semble impossible de démontrer qu'un ensemble donné ne correspond pas à une sous-droite projective de $PG(4, q')$, pour $q' > q$. Ceci étant dit, pour limiter le temps de calcul, c'est-à-dire pour que l'heuristique se termine, certains choix doivent être fait. En particulier, si l'ordre de l'ensemble doublement orthogonal recherché est J alors les géométries construites, conformément à l'algorithme 2.2, sont $PG(4, q)$ et $PG(4, q')$, q et q' étant les deux premières puissances d'entier premier supérieures à J.

Pour la seconde phase de notre méthode, c'est-à-dire la réduction, il est également important de faire certains choix pour les paramètres de l'algorithme 2.3. Pour la même raison que précédemment, le nombre potentiellement infini de droites projectives distinctes, il nous faut fixer les paramètres inhérents à la construction des géométries et aux droites utilisées. Tout d'abord, le premier paramètre qui doit être fixé est l'ordre des géométries projectives que nous considérerons. Pour appliquer l'algorithme 2.3 nous avons, dans tous les cas, utilisé uniquement la première puissance d'entier premier supérieure à l'ordre des ensembles voulus. Le second paramètre à considérer est la longueur des ensembles que nous utilisons pour appliquer la procédure de réduction. Dans la colonne intitulée *réduction* du Tableau 2.5, le nombre indiqué entre parenthèses correspond à la longueur maximale des ensembles

TABLEAU 2.5 – Comparaison des ensembles doublement orthogonaux.

# marques	réduction	géométrique	Haccoun
3	5	5	5
4	15(300)	17	15
5	41(430)	76	41
6	100(500)	155	100
7	211(1500)	387	222
8	435(2200)	692	459
9	891(3000)	1298	912
10	1646(6000)	2344	1698
11	3159(5500)	4052	3490
12	5038(8000)	5173	5173
13	8658(12000)	9482	8852
14	11347(15000)	11347	15596
15	20792(25000)	20848[a]	23193
16		25396[a]	36122
17		30387	50350
18		38426	75269
19		53657	110411
20		62345	156634
21		104310	212456
22		116314	293334
23		128609	391403
24		143280	534390
25		198899	709695
26		210825	940093
27		277146	1138060
28		301619	1490550
29		363589	1735395
30		412259	2494796

doublement orthogonaux obtenus de droites projectives que nous avons utilisées. Finalement, le dernier paramètre qu'il reste à fixer pour exécuter la procédure de réduction est le nombre d'itérations maximal que nous permettrons sans qu'il y ait d'amélioration de la longueur de l'ensemble doublement orthogonal présentement en cours. Ce paramètre appelé C_{max} dans l'algorithme 2.3, a été fixé à 15 dans notre

procédure. Aucune justification, autre qu'empirique, ne peut être donnée concernant ce choix, et il est probable qu'un autre choix ait donné des résultats distincts.

Finalement, le Tableau 2.6 donne les meilleurs ensembles doublement orthogonaux d'ordre 3 à 19, et le Tableau 2.7, les meilleurs ensembles d'ordre 20 à 30, obtenus par notre méthode.

TABLEAU 2.6 – Meilleurs ensembles doublement orthogonaux.

# marques	ensembles doublement orthogonaux
3	{0,1,5}
4	{0,2,12,15}
5	{0,1,24,37,41}
6	{0,1,17,70,95,100}
7	{0,4,34,81,195,206,211}
8	{0,22,30,114,263,414,432,435}
9	{0,6,41,346,632,649,817,849,891}
10	{0,4,108,446,456,1332,1347,1380,1615,1646}
11	{0,10,38,493,728,2020,2669,2698,3053,3107,3159}
12	{0,46,126,235,1306,1390,3398,3787,3840,4468,4709,5038}
13	{0,194,1836,2010,3789,4958,6941,7175,7216,7228,7908,8281,8658}
14	{0,900,1181,2038,3242,3565,6470,6510,9504,10544,11049,11181, 11342,11347}
15	{0,73,1304,1318,1459,3543,6462,7211,8410,9976,11176,12811, 18363,20462,20792}
16	{0,264,491,658,1090,3119,3904,10473,10555,10922,17008,21499, 23956,25281,25297,25824}
17	{0,495,3140,3734,6065,11740,14749,19102,19156,20831,21169, 21337,21342,23763,28887,29081,30387}
18	{0,2053,2746,3614,4784,10340,10800,11788,15935,16445,20523, 25522,29952,30626,32579,36519,37907,38426}
19	{0,30,872,873,1101,2733,14066,14847,25910,34006,35449,36090, 36619,37778,39117,42805,43570,50790,53657}

TABLEAU 2.7 – Meilleurs ensembles doublement orthogonaux (suite).

# marques	ensembles doublement orthogonaux
20	{0,495,1794,2464,4471,15409,19100,32872,35787,39553,42239, 42694,44731,45202,50330,54038,56420,57569,62140.62345}
21	{0,31,4338,5233,12757,17849,20126,21266,23092,23475,25738, 38183,48091,71564,72941,78850,80489,87849,101229,102848,104310}
22	{0,138,4425,4999,7984,10010,17859,25947,38839,46593,65248, 65773,84716,84827,85465,86347,100401,105208,109083,112600, 114936,116314}
23	{0,2565,3711,7817,15420,16761,25376,25868,46931,64855,64946, 78832,83534,83672,89333,99778,102798,113262,119734,121744, 124104,124213,128609}
24	{0,2582,16451,18106,22106,25650,32391,44120,45731,54136,66110, 85703,87934,94137,117151,125813,127873,130782,134985,135411, 136857,138197,141490,143280}
25	{0,834,1201,9514,18059,20790,44774,59094,60013,101230,102686, 105157,129350,131134,131311,147303,152882,163644,176041,177624, 181404,192333,192925,197515,198899}
26	{0,1384,5974,6566,17495,21275,22858,35255,46017,51596,67588, 67765,69549,93742,96213,97669,138886,139805,154125,178109, 180840,189385,197698,198065,198899,210825}
27	{0,4265,10791,17202,21895,30217,32025,37054,40943,42100,49793, 72305,77364,106458,111259,126176,142328,151899,207942,210617, 223240,228091,238319,247990,251846,253839,277146}
28	{0,156,570,22317,23059,36528,38871,49531,85565,91068,101439, 111230,135964,139507,140604,153887,156451,188536,214303,217796, 235876,256000,268275,274316,274568,277327,295758,301619}
29	{0,526,10698,17998,18085,39904,44178,64083,81869,86873,89493, 97949,106136,108045,114857,141742,181068,198065,281585,288546, 300582,301724,311314,321907,339026,346881,357759,359560, 363589}
30	{0,18561,19916,32442,40301,56578,76702,84219,98452,103333, 121993,151126,158883,163102,193933,216062,230747,254602,270504, 279774,282084,299391,342474,361303,361375,363167,366835,393075, 410261,412259}

CHAPITRE 3

PROBLÈME DU DTS

3.1 Généralités

3.1.1 Définition du problème

Définition 3.1. *Un (I, J)-DTS (Difference Triangle Set) est une famille*

$$\Delta = \{\Delta_1, \Delta_2, ..., \Delta_I\}$$

où les

$$\Delta_i = \{m_{ij} \mid 0 \leq j \leq J\}, \text{ pour } 1 \leq i \leq I$$

sont des ensembles d'entiers naturels tels que toutes les différences

$$m_{ij} - m_{ij'},$$

avec $1 \leq i \leq I$ et $0 \leq j' < j \leq J$, soient distinctes.

L'élément maximal d'un (I, J)-DTS Δ est noté $m(\Delta)$, autrement dit, on pose

$$m(\Delta) = \max\{m_{ij} | 0 \leq j \leq J, 1 \leq i \leq I\}.$$

Étant donné deux entiers I et J, le minimum de $m(\Delta)$, pour tous les Δ qui sont des (I, J)-DTS, est noté $M(I, J)$. Autrement dit, on pose

$$M(I, J) = \min\{m(\Delta) | \Delta \text{ est un } (I, J) - DTS\}.$$

Un DTS Δ qui satisfait $m(\Delta) = M(I, J)$ est dit *optimal.*

Lorsque Δ satisfait $m(\Delta) = M(I, J) = \frac{J(J+1)}{2} I$, c'est-à-dire que l'élément maximal du DTS est égal au nombre de différences générées, nous disons que Δ est un DTS *parfait.*

Exemple 3.2. *La famille* Δ *formée de*

$$\Delta_1 = \{0, 4, 6, 11\} \text{ et}$$
$$\Delta_2 = \{0, 1, 10, 13\}$$

est un (2,3)-DTS puisque les 12 différences possibles sont toutes distinctes. Pour cet exemple on a $m(\Delta) = 13$. *D'autre part, comme* $M(2, 3) = 13$, *on sait que* Δ *est un DTS optimal, mais ce DTS n'est pas parfait puisqu'il y a 12 différences générées et* $m(\Delta) = 13$. *En fait, puisque* Δ *est optimal, il est évident qu'il n'existe pas de* $(2, 3)$*-DTS parfait.*

Le problème qui consiste à déterminer un DTS optimal est généralement appelé problème du DTS. On peut remarquer que lorsque $I = 1$, c'est-à-dire que le DTS ne contient qu'un seul ensemble d'entiers, le problème est équivalent au problème de la règle de Golomb. En fait, on voit que le problème du DTS est une généralisation directe du problème de la règle de Golomb, puisqu'il s'agit de trouver un ensemble de règles de Golomb telles que les différences générées par les ensembles d'entiers soient toutes distinctes. Pour désigner un élément d'un DTS nous utiliserons donc, à l'occasion, le terme règle de Golomb ou simplement règle s'il n'y a pas d'ambiguïté.

3.1.2 Équivalences entre les DTS

Comme pour les règles de Golomb, il est possible de déterminer différentes classes d'équivalences induites par les symétries sur les différents DTS. Cette notion d'équivalence entre differents DTS s'avère importante à considérer au niveau de la résolution du problème, puisqu'il est alors possible d'éliminer plusieurs cas redondants, c'est-à-dire les règles équivalentes.

Comme nous l'avons déjà dit, un DTS est un ensemble de règles de Golomb. Il est donc évident que la symétrie relative aux règles de Golomb s'applique dans le cas des DTS. Pour toute règle de Golomb $\{a_1 = 0, a_2, \ldots, a_J\}$ la règle symétrique est $\{a_J - a_1, a_J - a_2, \ldots, a_J - a_J = 0\}$. Ces deux règles seront donc considérées équivalentes dans le problème du DTS. Notons que les différences générées par deux règles symétriques sont les mêmes ; cette remarque nous sera utile un peu plus loin.

Puisqu'un DTS est un ensemble, il n'existe pas d'ordre a priori sur ses éléments. Toutefois, il peut s'avérer avantageux, pour la résolution du problème, de considérer un tel ordre. En effet, lorsque $I > 1$, il est possible d'interchanger deux règles de Golomb. Il s'agit alors du même ensemble, mais la reconnaissance de ce fait n'est pas évidente de prime abord. Pour contrer cet effet, il est donc nécessaire dans certain cas de se munir d'une convention pour l'écriture des DTS, c'est-à-dire de fixer un ordre sur les éléments du DTS. Par exemple, on peut fixer l'ordre par rapport à l'élément maximal de chaque règle, ou encore selon l'élément minimal non nul de chaque règle. Les avantages de ces conventions varient selon la méthode de résolution adoptée.

En adoptant un représentant de classe pour chaque paire de règles de Golomb symétriques et en se fixant un ordre pour les éléments des DTS, il est possible de simplifier la reconnaissance des DTS équivalents et de réduire l'ensemble des solutions à considérer pour résoudre le problème.

3.1.3 Applications des DTS

Les applications des DTS à la vie courante sont très variées. Cette grande variété dans les champs d'application des DTS est principalement due aux $(1, J)$-DTS. Toutefois, en excluant les $(1, J)$-DTS, c'est-à-dire les règles de Golomb, les applications actuelles des DTS, bien que restreintes à la théorie des communications, demeurent importantes. En effet, plusieurs types de codes correcteurs d'erreurs sont construits à l'aide des DTS.

Robinson et Bernstein (1967) ont donné une construction, à partir de DTS, pour les codes convolutionnels auto-orthogonaux (CSOC, Convolutional Self-Orthogonal Codes), introduits par Massey (1963). Klieber (1970), Wu (1975; 1976) et Martin (1985) ont poursuivi les travaux pour cette application.

Chen, Fan et Jin (1992) ont fourni des constructions pour les codes quasi-cycliques auto-orthogonaux (SOQC, Self-Orthogonal Quasi-Cyclic Codes) qui ont été introduits par Townsend et Weldon (1967). Les mêmes auteurs mentionnent également les relations existant entre les codes optiques orthogonaux (OOC, Optical Orthogonal Codes) et les DTS.

Chu et Golomb (2003) ont récemment montré l'équivalence entre les DTS et les codes optiques orthogonaux stricts (SOOC, Strict Optical Orthogonal Codes), introduits par Zhang (1999).

3.1.4 Quelques résultats

Le problème du DTS est un problème NP-complet. Toutefois, pour certaines valeurs de J, le problème peut être résolu.

Théorème 3.3. *Pour $I \geq 1$, on a*

$$M(I,1) = I.$$

$$M(I,2) = \begin{cases} 3n, & si\ n \equiv 0\ ou\ 1 \mod 4 \\ 3n+1, & si\ n \equiv 2\ ou\ 3 \mod 4. \end{cases}$$

Il existe une infinité de valeurs de I pour lesquelles $M(I,3) = 6I$.

Pour $J = 1$ le résultat est trivial. La valeur de $M(I,2)$ provient de l'existence de certaines suites introduites par Skolem (1957) et Langford (Davies, 1959).

Le résultat pour $M(I,3)$ provient des travaux de Kotzig et Turgeon (1979) et Rogers (1981). Bermond a formulé la conjecture suivante concernant la valeur de $M(I,3)$.

Conjecture 3.4. *(Bermond, 1979) Pour tout $I \geq 4$, on a*

$$M(I,3) = 6I.$$

Cette conjecture a été vérifiée pour $4 \leq I \leq 22$ par Huang et Skiena (1994). Pour $J = 1,2,3$, il existe une infinité de (I,J)-DTS parfaits. Pour $J = 4$, nous connaissons également quelques $(I,4)$-DTS parfaits. Le résultat suivant, qui est une condition nécessaire pour qu'un DTS soit parfait, résume bien la situation (Bermond et al., 1976; Laufer, 1982).

Théorème 3.5. *Un (I,J)-DTS est parfait seulement si $J \leq 3$, ou $J = 4$ et $I \geq 6$ est un entier pair.*

En remarquant qu'un (I,J)-DTS contient exactement $IJ(J+1)/2$ différences distinctes on obtient évidemment la borne inférieure suivante :

$$M(I,J) \geq \frac{IJ(J+1)}{2},$$

appelée *borne inférieure triviale* du (I,J)-DTS.

Kløve a obtenu analytiquement des bornes inférieures sur la valeur de $M(I,J)$. Celles-ci sont resumées dans les deux théorèmes suivants.

Théorème 3.6. *(KlØve, 1988) Pour tout I et J on a*

$$M(I,J) \geq I\left(J^2 - 2J\sqrt{J} + \frac{J+\sqrt{J}}{4}\right).$$

Théorème 3.7. *(KlØve, 1989) Pour tout t, $t \leq J/2+1$, on a*

$$M(I,J) \geq \frac{1}{6}\{(2t^2-2t+3)I+(2t-5)\} + \frac{1}{t+1}\left(J-\frac{t-1}{2}\right)\left(tJI-\frac{t(t-1)}{2}I+1\right)+\frac{D}{3t(t+1)}, \text{ où}$$

$$\begin{array}{ll} D=0, & \text{pour } t=1 \text{ ou } I=1, \\ D=6I-6, & \text{pour } t=2, I\geq 2, \\ D=18I-24, & \text{pour } t=3, I\geq 2, \\ D=(9I-12)(t-1), & \text{pour } t\geq 4, 2\leq I\leq 8 \text{ et} \\ D=(10I-20)(t-1), & \text{pour } t\geq 4, I\geq 9. \end{array}$$

Mises à part quelques exceptions la borne du théorème 3.7 est toujours la meilleure borne analytique, c'est-à-dire obtenue d'une formule close.

Les meilleures bornes inférieures pour la valeur de $M(I,J)$ connues à ce jour restent celles obtenues par Shearer (1999) grâce à la programmation linéaire.

En ce qui concerne les bornes supérieures pour le problème du DTS, nous mentionnerons simplement, puisque ce sujet est abordé dans le reste de ce texte, qu'elles sont généralement obtenues par construction des DTS.

3.1.5 Différentes approches

Pour résoudre le problème du DTS, plusieurs approches ont été tentées. Dans ce qui suit, nous présenterons dans le détail ces différentes approches.

Une première approche consiste à utiliser les méthodes dites exactes. Dans ce genre d'approche on tente de fabriquer des DTS en tirant profit de certaines connaissances acquises en cours de construction, que se soient des bornes ou des caractéristiques particulières du problème. Toutefois, le problème étant très difficile, ces méthodes sont d'une utilité limitée.

Une autre approche utilise les techniques dites algébriques. Comme pour le problème des règles de Golomb, les propriétés de certaines structures algébriques ou combinatoires sont mises à profit pour créer de nouveaux DTS. Contrairement aux méthodes exactes, ces méthodes sont généralement rapides. Par contre, on ne peut habituellement rien dire au sujet de l'optimalité des solutions trouvées, à l'inverse des méthodes exactes.

Lorentzen et Nilsen (1991) ont pour leur part utilisé la programmation linéaire pour résoudre le problème du DTS. C'est à partir de ces travaux de Lorentzen et Nilsen que Shearer a pu déterminer les bornes inférieures mentionnées ci-dessus.

Suite aux tavaux mentionnés, nous proposons nous-même, d'une part, une approche basée sur la génération de colonnes et, d'autre part, une approche mixte qui tente de combiner les avantages de la génération de colonnes et des méthodes algébriques.

3.2 Approche algébrique

Dans cette section nous présentons tout d'abord différentes structures combinatoires s'apparentant fortement aux DTS, qui sont utilisées pour trouver de nouveaux DTS. Nous présentons ensuite, dans le détail, les principales techniques algébriques connues.

3.2.1 Quelques définitions

Définition 3.8. *Un (k, t, ν)-DDS (Disjoint Difference Set) est une famille*

$$\{B_f \mid f \in F\}$$

de t sous-ensembles de $\mathbb{Z}_\nu$, les entiers modulo ν, chacun de cardinalité k, telle que toutes les différences non nulles de l'ensemble

$$\{(a-b) \mod \nu \mid a, b \in B_f; a \neq b; f \in F\}$$

sont distinctes.

Pour $t = 1$, nous utiliserons la notation (k, ν)-DDS ou $(k, 1, \nu)$-DDS. Un (k, ν)-DDS est en fait ce que nous avons appelé auparavant un CDS modulo ν d'ordre k.

Exemple 3.9. *La famille formée de*

$$B_1 = \{0, 4, 6, 11\} \text{ et}$$
$$B_2 = \{0, 1, 10, 13\}$$

est un (4,2,27)-DDS. On peut effectivement vérifier que les 24 différences non nulles générées sont toutes distinctes modulo 27.

Lemme 3.10. *(Atkinson et al., 1986) Soit $X = \{X_1, X_2, ..., X_t\}$ un (k, t, ν)-DDS. Si $Y_i = mX_i + r_i$ avec $\gcd(m, \nu) = 1$ et $r_i \in \mathbb{Z}_\nu$, $1 \leq i \leq t$, alors $Y = \{Y_1, Y_2, ..., Y_t\}$ est aussi un (k, t, ν)-DDS.*

On vérifie facilement qu'un (I, J)-DTS est aussi un $(J+1, I, \nu)$-DDS, pour ν suffisamment grand, et qu'un (J, I, ν)-DDS forme aussi un $(I, J-1)$-DTS. En effet, un (J, I, ν)-DDS considéré sans le module ν est nécessairement un $(I, J-1)$-DTS puisque toutes les différences positives doivent être distinctes. Inversement, étant donné un (I, J)-DTS Δ, il suffit de prendre $\nu = 2m(\Delta) + 1$ comme module pour obtenir un $(J+1, I, \nu)$-DDS. En effet, les différences générées étant les différences du DTS et ν moins les différences du DTS, elles sont donc toutes distinctes modulo ν. Par exemple, si on ne considère pas le module du (4,2,27)-DDS de l'exemple 3.9, on obtient le (2,3)-DTS de l'exemple 3.2 et vice versa.

Définition 3.11. *Un BIBD (Balanced Incomplete Block Design) est un arrangement de ν objets distincts en b blocs tel que chaque bloc contient exactement k objets différents, chaque objet apparaissant dans exactement r blocs différents, et chaque paire d'objets distincts apparaissant ensemble dans exactement λ blocs. Un tel design de blocs est appelé un (ν, b, r, k, λ)-BIBD.*

Un BIBD cyclique peut être représenté comme un BIBD ayant pour objets les entiers de $\mathbb{Z}_\nu$, et tel que si $\{a_1, a_2, ..., a_k\}$ est un bloc alors $\{a_1 + 1, a_2 + 1, ..., a_k + 1\}$ (avec l'addition modulo ν) est aussi un bloc.

Exemple 3.12. *L'ensemble des blocs suivant forment un $(13, 26, 8, 4, 2)$-BIBD :*

0	1	4	6	0	1	5	9
1	2	5	7	0	2	6	10
2	3	6	8	0	3	7	11
3	4	7	9	0	4	8	12
4	5	8	10	1	2	7	12
5	6	9	11	1	4	6	11
6	7	10	12	1	3	8	10
7	8	11	0	2	3	4	5
8	9	12	1	2	9	11	8
9	10	0	2	3	6	9	12
10	11	1	3	4	7	9	10
11	12	2	4	5	6	7	8
12	0	3	5	5	10	11	12.

Ce BIBD n'est pas cyclique puisque le bloc $\{0, 1, 5, 9\}$ appartient au BIBD et le bloc $\{1, 2, 6, 10\}$ n'y apparaît pas.

Dans un BIBD cyclique, l'automorphisme $\sigma : a \to a + 1 \mod \nu$ partitionne les b blocs en classes d'équivalence. Un ensemble de *blocs de départ* est alors un ensemble de représentants pour ces classes et un bloc de cet ensemble est dit *plein* s'il engendre ν blocs.

Exemple 3.13. *L'ensemble des blocs suivants forme un* $(6, 20, 10, 3, 4)$*-BIBD cyclique :*

0	1	2	0	1	3	0	1	4	0	2	4
1	2	3	1	2	4	1	2	5	1	3	5.
2	3	4	2	3	5	2	3	0			
3	4	5	3	4	0	3	4	1			
4	5	0	4	5	1	4	5	2			
5	0	1	5	0	2	5	0	3			

Les blocs ci-dessus sont partitionnés en classes d'équivalence, chaque colonne représentant une classe. Si on prend comme représentants le premier bloc de chaque colonne, on obtient les 4 blocs de départs : $\{0, 1, 2\}$, $\{0, 1, 3\}$, $\{0, 1, 4\}$ *et* $\{0, 2, 4\}$. *Les trois premiers blocs sont pleins puisqu'ils engendrent chacun 6 blocs et le bloc* $\{0, 2, 4\}$ *n'est pas plein puisqu'il n'engendre que 2 blocs.*

À partir d'un $(\nu, b, r, k, 1)$-BIBD cyclique, si on prend les blocs de départ pleins comme ensembles de différences, on obtient un (k, t, ν)-DDS, où $t = \lfloor r/k \rfloor$.

Exemple 3.14. *Les ensembles*

$$D_1 = \{0, 10, 27, 28, 31, 43, 50\},$$
$$D_2 = \{0, 11, 20, 25, 49, 55, 57\}, \text{ et}$$
$$D_3 = \{0, 13, 26, 39, 52, 65, 78\}$$

sont trois blocs de départ pour un $(91, 195, 15, 7, 1)$*-BIBD cyclique. Les blocs* D_1 *et* D_2 *engendrent 91 blocs chacun et le bloc* D_3 *engendre 13 blocs.* D_1 *et* D_2 *sont des blocs pleins et ainsi* $\{D_1, D_2\}$ *est un* $(7, 2, 91)$*-DDS.*

3.2.2 Méthode de Kløve

Cette méthode, due à Kløve (1989), nous permet de construire des DTS à partir d'un DDS.

Soit $\{m_i \mid 0 \leq i \leq k-1\}$ un (k, ν)-DDS et soit $S = \{S_1, S_2, ..., S_I\}$ une famille de sous-ensembles de $\{0, 1, ..., k-1\}$ de cardinalité $J+1$ telle que $|S_i \cap S_{i'}| \leq 1, \forall i, i'$. Notons $s_{i0} < s_{i1} < ... < s_{iJ}$ les éléments de S_i et $\Delta_i = \{m_{s_{ij}} - m_{s_{i0}} \mid 0 \leq j \leq J\}$. Alors

$$\Delta = \{\Delta_i \mid 1 \leq i \leq I\}$$

est un (I, J)-DTS.

Exemple 3.15. $\{0, 4, 11, 20, 25, 26, 28, 38\}$ *est un (8,57)-DDS.*

Soit $S = \{S_1 = \{0, 1, 2, 3\}, S_2 = \{4, 5, 6, 7\}\}$. *On a*

$$\begin{array}{ll} 0-0=0 & 25-25=0 \\ 4-0=4 & 26-25=1 \\ 11-0=11 & 28-25=3 \\ 20-0=20 & 38-25=13, \end{array}$$

et ainsi

$$\{\{0, 4, 11, 20\}, \{0, 1, 3, 13\}\}$$

est un (2,3)-DTS.

Soit $S = \{S_1 = \{0, 1, 2\}, S_2 = \{4, 6, 7\}\}, S_3 = \{3, 5, 7\}$. *On a*

$$\begin{array}{lll} 0-0=0 & 25-25=0 & 20-20=0 \\ 4-0=4 & 28-25=3 & 26-20=6 \\ 11-0=11 & 38-25=13 & 38-20=18, \end{array}$$

et ainsi

$$\{\{0, 4, 11\}, \{0, 3, 13\}, \{0, 6, 18\}\}$$

est un (3,2)-DTS.

La méthode de Kløve est un cas particulier de la construction ci-dessus. Si $\{p_i | 1 \leq i \leq I\}$ est une suite d'entiers telle que

- $p_1 \geq 0$,
- $p_{i+1} - p_i \geq J$ pour $1 \leq i \leq I$ et
- $p_I < n - J$,

alors on peut choisir $S_i = \{p_i, p_i + 1, ..., p_i + J\}$. Ce qui donne

$$\Delta = \{\{c_j - c_{p_i} | p_i \leq j \leq p_i + J\} | 1 \leq i \leq I\}$$

et

$$m(\Delta) = \max_{1 \leq i \leq I} \{c_{p_i+J} - c_{p_i}\}.$$

Exemple 3.16. *Pour $I = 2$, $J = 3$ et le (8,57)-DDS de l'exemple 3.15, les suites $\{p_i | 1 \leq i \leq I\}$ possibles sont $\{0, 3\}$, $\{0, 4\}$ et $\{1, 4\}$. On obtient respectivement,*

$$S = \{S_1 = \{0, 1, 2, 3\}, S_2 = \{3, 4, 5, 6\}\},$$
$$S = \{S_1 = \{0, 1, 2, 3\}, S_2 = \{4, 5, 6, 7\}\},$$
$$S = \{S_1 = \{1, 2, 3, 4\}, S_2 = \{4, 5, 6, 7\}\},$$

qui nous donnent les trois (2,3)-DTS suivants

$$\{\{0, 4, 11, 20\}, \{0, 5, 6, 8\}\},$$
$$\{\{0, 4, 11, 20\}, \{0, 1, 3, 13\}\},$$
$$\{\{0, 3, 10, 19\}, \{0, 1, 3, 13\}\}.$$

3.2.3 Méthode de Chen, Fan et Jin

Cette méthode, due à Chen, Fan et Jin (1992), nous permet de générer des nouveaux DDS à partir d'un DDS initial.

Étant donné un (k, t, ν)-DDS, $\nu \not\equiv 0 \mod k$, si $\gcd(r, (k-1)!) = 1$ alors on construit un $(k, rt, r\nu)$-DDS de la manière suivante. Pour chaque ensemble de différences $\{0, d_1, ..., d_{k-1}\}$ du DDS, on prend les r ensembles de différences $\{0, d_1 + i\nu, d_2 + 2i\nu, ..., d_{k-1} + (k-1)i\nu\}$, $0 \leq i < r$, en considérant les additions modulo νr.

De plus, s'il existe un (k, t', r)-DDS D', alors on peut construire un $(k, rt + t', r\nu)$-DDS en ajoutant les t' ensembles de différences $\{0, \nu s_1, ..., \nu s_{k-1}\}$ obtenus de $D'_i = \{0, s_1, ..., s_{k-1}\}$ pour $D' = \{D'_i | 1 \leq i \leq t'\}$.

Exemple 3.17. *Soit* $\{0,1,4,6\}$ *un* $(4,1,13)$*-DDS. Puisque* $13 \not\equiv 0 \mod 4$ *et que* $\gcd(5,4!) = 1$, *on peut construire le* $(4,5,65)$*-DDS suivant.*

$$\begin{array}{ll} i{=}0: & \{0,1,4,6\} \\ i{=}1: & \{0,14,30,45\} \\ i{=}2: & \{0,27,56,19\} \\ i{=}3: & \{0,40,17,58\} \\ i{=}4: & \{0,53,43,32\}. \end{array}$$

Il n'existe pas de $(4,t',5)$*-DDS, et ainsi la dernière partie de la construction ne peut pas s'appliquer. En fait, pour que cette partie de la construction s'applique, il faut que l'entier* r *soit suffisamment grand, c'est-à-dire que* r *doit être le module d'un* $(4,t',5)$*-DDS.*

3.2.4 Méthode de Ling

Cette méthode, due à Ling (2002), nous permet de construire des DTS à partir des DDS obtenus du plan semi-affine.

Notons D_q le $(q,1,q^2-1)$-DDS obtenu du plan semi-affine d'ordre q et

$$R_q = \{0, q+1, 2(q+1), ..., (q-2)(q+1)\}.$$

Soit $q+1 = ab$. On définit

$$Y_i = \{x - i | x \in D_q, x \equiv i \mod a\}$$

pour $i = 0,1,2,...,a-1$. On a ainsi, $a-1$ ensembles Y_i de cardinalité b et un de ces ensembles est de cardinalité $b-1$. De plus, tous les éléments des Y_i sont des multiples de a. En divisant les éléments des Y_i par a et en soustrayant, pour tous les Y_i, le plus petit entier à chaque élément, on obtient des ensembles de différences générant exactement une fois tous les entiers de $\mathbb{Z}_{b(q-1)}$ qui ne sont pas multiple de b.

En ôtant l'élément maximum de chaque Y_i de cardinalité b, on obtient avec cette méthode un nouveau $(b-1, a, b(q-1))$-DDS. Il est évidemment possible de construire un $(k, a, b(q-1))$-DDS, $k < b-1$, en otant les $b-k-1$ plus grands éléments de chaque ensemble de différences.

Après avoir construit un $(k, a, b(q-1))$-DDS, puisqu'aucune différence engendrée par cette méthode n'est un multiple de b, alors, s'il existe un $(k-1, t')$-DTS D', on peut construire un $(k, a+t')$-DTS en ajoutant les t' ensembles de différences $\{0, bs_1, ..., bs_{k-1}\}$ obtenus de $D'_i = \{0, s_1, ..., s_{k-1}\}$ pour $D' = \{D'_i | 1 \leq i \leq t'\}$.

Exemple 3.18. *Pour $q = 7$, on a $R_7 = \{0, 8, 16, 24, 32, 40\}$. Soit*

$$D_7 = \{0, 6, 9, 10, 21, 23, 28\}$$

le $(7, 1, 48)$-DDS obtenu du plan semi-affine d'ordre 7. On a que $q+1 = 8$, posons $a = 2$ et $b = 4$. On obtient

$$\begin{aligned} Y_0 &= \{x - 0 | x \in D_7, x \equiv 0 \mod 2\} = \{0, 6, 10, 28\} \\ Y_1 &= \{x - 1 | x \in D_7, x \equiv 1 \mod 2\} = \{8, 20, 22\}, \end{aligned}$$

d'où,

$$\{\{0, 3, 5\}, \{0, 6, 7\}\}$$

est un $(3, 2, 24)$-DDS, de même qu'un $(2, 2)$-DTS.

Puisque $\{0, 1, 3\}$ est un $(2, 1)$-DTS, on peut dans ce cas ajouter au DTS précédent, l'ensemble $\{0, 4, 12\}$, et ainsi obtenir le $(2, 3)$-DTS suivant :

$$\{\{0, 3, 5\}, \{0, 6, 7\}, \{0, 4, 12\}\}.$$

3.2.5 Méthode de Mathon

Cette méthode, due à Mathon (1987), nous permet de générer des DDS à partir de paires d'entiers premiers.

Soient $k = 2m + 1$ et $p = 2mt + 1$, $t \geq 2$, deux entiers premiers et soit α une racine primitive de $\mathbb{Z}_p$. On définit $m - 1$ nombres r_i par les équations $\alpha^{r_i} = \alpha_{ti} - 1$, $i = 1, 2, ..., m - 1$. S'il existe $\beta \in \mathbb{Z}_k$ tel que les $2m$ éléments ± 1, $\pm(\beta^{ti} - 1)\beta^{-r_i}$, $i = 1, 2, ..., m - 1$ soient tous distincts dans $\mathbb{Z}_k$, alors les blocs

$$D_{i+1} = \{0_0, \alpha^i_{\beta^i}, \alpha^{t+i}_{\beta^{t+i}}, ..., \alpha^{2mt-t+i}_{\beta^{2mt-t+i}}\},\ i = 0, 1, ..., t - 1$$

forment un (k, t, kp)-DDS. La notation utilisée étant $\alpha^i_{\beta^j} = k\alpha^i + p\beta^j$.

Exemple 3.19. *Prenons $k = 2m + 1 = 7$, si on choisit $p = 2mt + 1 = 13$ alors il existe une solution. En effet, $2 \in \mathbb{Z}_{13}$ est une racine primitive. On a les $m - 1 = 2$ nombres, r_1 tel que $\alpha^{r_1} = \alpha_2 - 1$ et r_2 tel que $\alpha^{r_2} = \alpha_4 - 1$, c'est-à-dire, après calcule $r_1 = 4$ et $r_2 = 1$. Prenant $\beta = 2 \in \mathbb{Z}_7$, on obtient*

$$\{\pm 1, \pm(2^2 - 1)2^{-4}, \pm(2^4 - 1)2^{-1}\} = \{\pm 1, \pm 5, \pm 4\}$$

qui sont tous distincts dans $\mathbb{Z}_7$. Ainsi,

$$\begin{aligned} \{0_0, 1_1, 4_4, 3_2, 12_1, 9_4, 10_2\} &= \{0, 20, 80, 47, 6, 24, 5\} \\ \{0_0, 2_4, 8_1, 6_4, 11_2, 5_1, 7_4\} &= \{0, 40, 69, 3, 12, 48, 10\} \end{aligned}$$

forment un $(7, 2, 91)$-DDS.

3.2.6 Méthode de Chen

Cette méthode, due à Chen (1994), nous permet de construire des DTS à partir d'un ASP (Additive Sequence of Permutations).

Définition 3.20. *Soit X^1 le $(2r + 1)$-vecteur $(-r, -r + 1, ..., -1, 0, 1, ..., r - 1, r)$ et soient $X^2, ..., X^n$ des permutations de X^1. On dit que $(X^1, X^2, ..., X^n)$ est un ASP d'ordre $2r + 1$, et de longueur n, si le vecteur somme de toute sous-suite $X^i, X^{i+1}, ..., X^{i+t}$ de permutations consécutives est aussi une permutation de X^1.*

Définition 3.21. *Un triangle d'additions d'ordre n est une collection T de $\frac{n(n-1)}{2}$ entiers s_j^k, $k = 1, 2, ..., n$; $j = 1, 2, ..., n-k+1$, telle que*

$$s_j^k = \sum_{i=j}^{j+k-1} s_i^1.$$

On note s_j^k l'entrée à la position (k, j) de T. On peut représenter T sous la forme triangulaire suivante :

$$\begin{array}{ccccccccccc} s_1^1 & & s_2^1 & & \cdots & & s_{n-1}^1 & & s_n^1 & & \\ & s_1^2 & & s_2^2 & & \cdots & & s_{n-1}^2 & & & \\ & & \cdots & & \cdots & & \cdots & & & & \\ & & & s_1^{n-1} & & s_2^{n-1} & & & & & \\ & & & & s_1^n. & & & & & & \end{array}$$

En considérant les définitions ci-dessus, il est possible de voir qu'un ASP d'ordre $2r+1$, $(X^1, X^2, ..., X^n)$, génère $2r+1$ triangles d'additions d'ordre n ayant pour entrée les entiers de X^1. En effet, notons $X_j^i = \sum_{k=j}^{i} X^k$, $i \geq j$, et représentons l'ASP selon le triangle d'addition,

$$\begin{array}{ccccccccccc} X_1^1 & & X_2^2 & & X_3^3 & & \cdots & & X_n^n & & \\ & X_1^2 & & X_2^3 & & \cdots & & X_{n-1}^n & & & \\ & & \cdots & & \cdots & & \cdots & & & & \\ & & & X_1^{n-1} & & X_2^n & & & & & \\ & & & & X_1^n, & & & & & & \end{array}$$

alors chaque entrée du triangle est, par définition, une permutation de X^1. En prenant pour chaque entrée du triangle le k-ième terme de la permutation, on obtient ainsi un triangle d'additions avec pour entrées les entiers de X^1. Puisqu'il est possible de faire de même pour chacune des $2r+1$ positions, on a bien $2r+1$ triangles d'additions.

Soit $\Delta = \{\Delta_1, \Delta_2, ..., \Delta_I\}$ un (I, J)-DTS. Chaque Δ_i détermine un triangle d'additions d'ordre J avec pour entrées $s_j^k = a_{i,j+k} - a_{ij}$, pour $k = 1, 2, ..., J$ et $j = 1, 2, ..., J-k+1$.

Soient $U_1, U_2, ..., U_{2r+1}$, les triangles d'additions correspondant à un ASP d'ordre $2r+1$ et de longueur J. Soient $T_1, T_2, ..., T_I$ les triangles d'additions correspondant

à un (I, J)-DTS. Pour $i = 1, 2, ..., I$ et $j = 1, 2, ..., 2r + 1$, on définit les triangles d'additions $T_i + U_j$ comme suit : pour $k = 1, 2, ..., J$ et $p = 1, 2, ..., J - k + 1$, l'entrée en position (k, p) de $T_i + U_j$ est $(2r + 1)t_p^k + u_p^k$, où T_i a l'entrée t_p^k et U_j a l'entrée u_p^k en position (k, p). Les $(2r + 1)I$ triangles d'additions ainsi construits forment donc un nouveau $((2r + 1)I, J)$-DTS avec pour valeur maximale $m = (2r + 1)m_1 + r$, où m_1 est l'élément maximal du (I, J)-DTS de départ.

Exemple 3.22. *Un (3, 4)-DTS est donné par*

$$\Delta_1 = \{0, 9, 14, 26, 32\},$$
$$\Delta_2 = \{0, 8, 10, 29, 30\}, \text{ et}$$
$$\Delta_3 = \{0, 4, 15, 28, 31\}.$$

Les 3 triangles d'additions générés par ce DTS sont

9		5		12		6	8		2		19		1	
	14		17		18			10		21		20		
		26		23					29		22			
			32							30				

4		11		13		3
	15		24		16	
		28		27		
			31			

Un ASP d'ordre 5 et de longueur 4 est donné par

$$X^1 = (-2, -1, 0, 1, 2),$$
$$X^2 = (0, 1, 2, -2, -1),$$
$$X^3 = (2, -2, -1, 0, 1), \text{ et}$$
$$X^4 = (-1, 0, 1, 2, -2).$$

Les 5 triangles d'additions générés par cet ASP sont

$$\begin{array}{cccccccc|cccccccc}
-2 & & 0 & & 2 & & -1 & & -1 & & 1 & & -2 & & 0 & \\
& -2 & & 2 & & 1 & & & & 0 & & -1 & & -2 & & \\
& & 0 & & 1 & & & & & & -2 & & -1 & & & \\
& & & -1 & & & & & & & & -2 & & & & \\
\hline
0 & & 2 & & -1 & & 1 & & 1 & & -2 & & 0 & & 2 & \\
& 2 & & 1 & & 0 & & & & -1 & & -2 & & 2 & & \\
& & 1 & & 2 & & & & & & -1 & & 0 & & & \\
& & & 2 & & & & & & & & 1 & & & & \\
\hline
& & & & 2 & & -1 & & 1 & & -2 & & & & & \\
& & & & & 1 & & 0 & & -1 & & & & & & \\
& & & & & & 2 & & -2 & & & & & & & \\
& & & & & & & 0 & & & & & & & &
\end{array}$$

Ainsi le triangle d'additions correspondant à $T_1 + U_1$ est

$$\begin{array}{ccccccccc}
5*9-2 & & 5*5+0 & & 5*12+2 & & 5*6-1 \\
& 5*14-2 & & 5*17+2 & & 5*18+1 & \\
& & 5*26+0 & & 5*23+1 & & \\
& & & 5*32-1, & & &
\end{array}$$

c'est-à-dire,

$$\begin{array}{ccccccc}
43 & & 25 & & 62 & & 29 \\
& 68 & & 87 & & 91 & \\
& & 130 & & 116 & & \\
& & & 159. & & &
\end{array}$$

L'ensemble du DTS correspondant à ce triangle est alors

$$\{0, 43, 68, 130, 159\}.$$

En faisant de même pour chaque $T_i + U_j$, $i = 1, 2, 3$; $j = 1, 2, 3, 4, 5$, on obtient les 15 ensembles formant un $(15, 4)$-DTS ayant pour élément maximal la valeur $5*32+2 =$ 162.

Des méthodes de construction pour les ASP sont présentées dans deux articles de Kotzig et Turgeon (1979; 1982).

3.3 Formulation à l'aide de la programmation linéaire

La formulation du problème du DTS sous forme d'un problème de programmation linéaire (en nombres entiers) est due à Lorentzen et Nilsen (1991). Nous présentons dans cette section la formulation du problème en programmation linéaire. Nous discutons ensuite des améliorations du modèle, apportées par les auteurs ainsi que par Shearer (1999), pour le calcul de la borne inférieure sur $M(I, J)$. Puis nous terminons cette section avec les résultats obtenus par cette approche.

3.3.1 Formulation initiale

Soit m_{ij} la j-ème marque de la i-ème règle de Golomb d'un (I, J)-DTS. Notons $\delta_{ijj'k}$ la variable 0-1 qui est égale à 1 si $m_{ij'} - m_{ij} = k$ et à 0 sinon, où $1 \leq k \leq K$, pour K une borne supérieure connue pour $M(I, J)$. Le problème de déterminer un (I, J)-DTS optimal peut alors s'exprimer comme suit :

Formulation PNE

Minimisez z sous les contraintes :

$$z \geq m_{iJ}, \qquad 1 \leq i \leq I; \tag{3.1}$$

$$m_{ij'} - m_{ij} = \sum_{k=1}^{K} k\delta_{ijj'k}, \qquad 1 \leq i \leq I,\ 0 \leq j < j' \leq J; \tag{3.2}$$

$$\sum_{k=1}^{K} \delta_{ijj'k} = 1, \qquad 1 \leq i \leq I,\ 0 \leq j < j' \leq J; \tag{3.3}$$

$$\sum_{i=1}^{I} \sum_{j<j'} \delta_{ijj'k} \leq 1, \qquad 1 \leq k \leq K; \tag{3.4}$$

$$m_{i0} = 0, \qquad 1 \leq i \leq I;$$

$$\delta_{ijj'k} \in \{0, 1\}.$$

La relaxation continue de ce problème en nombres entiers est facile à résoudre en principe, et la valeur optimale de la fonction objectif z constitue une borne inférieure pour $M(I, J)$. Toutefois, lorsque les paramètres I et J deviennent assez grands, le nombre de variables $\delta_{ijj'k}$ devient exorbitant. Pour contrer ce problème les auteurs proposent quelques modifications au modèle leur permettant d'ajouter de façon dynamique les contraintes nécessaires.

3.3.2 Formulation revisée

La formulation revisée du problème précédent consiste à ne considérer que les différences successives dans les contraintes (3.2)-(3.4) et ajouter de nouvelles contraintes pour tenir compte des différences entre les marques à distance deux ou plus.

Notons $\delta_{ijk} = \delta_{i,j,j+1,k}$. Ces nouvelles variables ne sont pas suffisantes pour décrire le problème, il faut donc ajouter de nouvelles contraintes au problème.

Soit $\{\ell_{ijj'k\nu}\}_{j\leq\nu\leq j'-1}$ un ensemble de $j'-j$ entiers distincts tel que $\sum_{\nu=j}^{j'-1}\ell_{ijj'k\nu}=k$, pour $j'>j+1$. Autrement dit, $\{\ell_{ijj'k\nu}\}_{j\leq\nu\leq j'-1}$ est une partition de k en $j'-j$ entiers distincts. Alors on a $\sum_{\nu=j}^{j'-1}\delta_{i\nu\ell_{ijj'k\nu}}\leq j'-j-1+\delta_{ijj'k}$, puisque $\sum_{\nu=j}^{j'-1}\delta_{i\nu\ell_{ijj'k\nu}}=j'-j$ implique $\delta_{ijj'k}=1$.

Soit S un sous-ensemble de $\{(i,j,j')\mid j<j'\}$. Alors $\sum_{(i,j,j')\in S}\delta_{ijj'k}\leq 1$ implique

$$\sum_{(i,j,j')\in S}\sum_{\nu=j}^{j'-1}\delta_{i\nu\ell_{ijj'k\nu}}\leq 1+\sum_{(i,j,j')\in S}(j'-j-1).$$

Avec ces nouvelles contraintes, la formulation en nombres entiers s'exprime alors comme suit :

Formulation PNE revisée

Minimisez z sous les contraintes :

$$z \geq m_{iJ}, \qquad 1 \leq i \leq I; \quad (3.5)$$

$$m_{i,j+1} - m_{ij} = \sum_{k=1}^{K} k\delta_{ijk}, \qquad 1 \leq i \leq I,\ 0 \leq j < J; \quad (3.6)$$

$$\sum_{k=1}^{K} \delta_{ijk} = 1, \qquad 1 \leq i \leq I,\ 0 \leq j < J; \quad (3.7)$$

$$\sum_{i=1}^{I} \sum_{j<J} \delta_{ijk} \leq 1, \qquad 1 \leq k \leq K; \quad (3.8)$$

$$\sum_{(i,j,j')\in S} \sum_{\nu=j}^{j'-1} \delta_{i\nu\ell_{ijj'k\nu}} \leq 1 + \sum_{(i.j.j')\in S} (j' - j - 1), \qquad \forall S \subseteq \{(i,j,j')|j < j'\}, \quad (3.9)$$

$$1 \leq k \leq K, \text{ et}$$

$$\forall \text{ partition } \{\ell_{ijj'k\nu}\} \text{ de } k;$$

$$m_{i0} = 0, \qquad 1 \leq i \leq I;$$

$$\delta_{ijk} \in \{0,1\}.$$

Proposition 3.23. *(Lorentzen et Nilsen, 1991) Les deux formulations en nombres entiers, ci-dessus, sont équivalentes.*

Preuve. Les contraintes (3.6) et (3.7) imposent que toutes les marques ainsi que toutes les différences entre deux marques successives aient une valeur unique. Puisqu'il est possible d'exprimer la différence entre deux marques quelconques comme une somme de différences successives, cela implique que toute différence entre deux marques quelconques a une valeur uniquement déterminée, ce qui est imposé par les contraintes (3.2) et (3.3). Les contraintes (3.6) et (3.7) sont donc équivalentes aux contraintes (3.2) et (3.3).

Les contraintes (3.4) imposent que les différences entre deux marques quelconques soient toutes distinctes alors que les contraintes (3.8) imposent que seulement les différences entre les marques successives soient distinctes. Il reste donc à montrer que les contraintes (3.9) sont suffisantes pour imposer que les différences entre deux marques quelconques soient toutes distinctes.

En effet, supposons qu'on ait deux fois la même différence générée. Alors il existe (i_1, j_1, j_1') tel que $m_{i_1 j_1'} - m_{i_1 j_1} = k$ et (i_2, j_2, j_2') tel que $m_{i_2 j_2'} - m_{i_2 j_2} = k$.

Puisque toutes les différences entre deux marques successives doivent être distinctes, il existe alors deux partitions de k en entiers distincts $\{\ell_{i_1 j_1 j_1' k\nu}\}_{j_1 \leq \nu \leq j_1'-1}$ et $\{\ell_{i_2 j_2 j_2' k\nu}\}_{j_2 \leq \nu \leq j_2'-1}$ telles que $\sum_{\nu=j_1}^{j_1'-1} \delta_{i_1 \nu \ell_{i_1 j_1 j_1' k\nu}} = j_1' - j_1$ et $\sum_{\nu=j_2}^{j_2'-1} \delta_{i_2 \nu \ell_{i_2 j_2 j_2' k\nu}} = j_2' - j_2$.

Ainsi, pour $S = \{(i_1, j_1, j_1'), (i_2, j_2, j_2')\}$, une des contraintes (3.9) est violée.

Puisque les contraintes (3.8) et (3.9) imposent que les différences entre deux marques quelconques soient distinctes, ces contraintes sont donc équivalentes aux contraintes (3.4).

□

Comme nous venons de le voir dans la preuve précédente, pour résoudre le problème en nombres entiers, il est suffisant de considérer, pour les contraintes (3.9), les sous-ensembles S de cardinalité 2. Toutefois, en considérant les sous-ensembles de cardinalité quelconque il est possible d'améliorer la borne inférieure sur $M(I, J)$. Une autre façon d'améliorer cette borne consiste à tenir compte des contraintes supplémentaires

$$\sum_{(i,j,j') \in S} (m_{ij'} - m_{ij}) \geq |S|(|S| + 1)/2. \tag{3.10}$$

Comme nous l'avons déjà mentionné, dans la formulation initiale le nombre de variables δ devient très grand lorsque I et J sont grands. Dans la formulation revisée, le nombre de variables est considérablement réduit, mais en contre partie le nombre de contraintes augmente beaucoup. Ce problème peut être évité si dans l'implémentation de cet algorithme, les contraintes (3.9) et (3.10) sont ajoutées de façon dynamique seulement lorsqu'elles deviennent nécessaires. Pour avoir plus d'information sur l'implémentation de cet algorithme le lecteur doit consulter l'article de Lorentzen et Nilsen (1991).

Les bornes inférieures pour $M(I, J)$ obtenues de cette méthode sont présentées à la table 3.1.

TABLEAU 3.1 – Bornes inférieures PNE pour $M(I, J)$ (Lorentzen et Nilsen).

J	$I = 1$	$I = 2$	$I = 3$	$I = 4$	$I = 5$
1	1	2	2	3	3
2	3	6	8	10	12
3	6	11	16	21	26
4	11	20	29	38	47
5	17	31	46	60	75
6	24	46	67	89	110
7	32	62	92	122	152
8	43	82	122	162	202
9	54	105	156	207	
10	67	131	195	258	
11	82	160	239		
12	98	193	287		
13	116	229			
14	136	268			
15	157	310			
16	180	355			
17	204	404			
18	230	456			
19	258	512			
20	287	570			

3.3.3 Amélioration du modèle revisé

Pour améliorer les bornes inférieures de $M(I,J)$, Shearer (1999) a introduit de nouvelles contraintes dans le modèle revisé de Lorentzen et Nilsen. Ces contraintes viennent de l'observation présentée dans le résultat suivant.

Lemme 3.24. *Soit S un ensemble de n entiers distincts, de moyenne r. Soit m l'élément maximum de S. Alors on a $m \geq r + (n-1)/2$.*

Preuve. (Shearer, 1999) Soit s la somme des éléments de S. On a $s = nr$. Puisque les éléments de S sont distincts et de maximum m, on a $s \leq m + (m-1) + \cdots + (m-n+1) = mn - \frac{(n-1)n}{2}$. Par conséquent, on a $nr \leq mn - \frac{(n-1)n}{2}$, ou encore, $m \geq r + (n-1)/2$. □

Notons $d^i_{j'j} = m_{ij'} - m_{ij}$, pour $0 \leq j < j' \leq J$. Cette notation permet d'écrire le triangle des différences pour la règle i de la manière suivante :

m_{i0}		m_{i1}		m_{i2}		m_{i3}		$\cdots$		$m_{i(J-1)}$		m_{iJ}
	d^i_{10}		d^i_{21}		d^i_{32}		$\cdots$		$\cdots$		$d^i_{J(J-1)}$	
		d^i_{20}		d^i_{31}		$\cdots$		$\cdots$		$d^i_{J(J-2)}$		
			d^i_{30}		$\cdots$		$\cdots$		$\cdots$			
				$\cdots$		$\cdots$		$\cdots$				
					$d^i_{(J-1)0}$		d^i_{J1}					
						d^i_{J0}						

On peut voir que $d^i_{j'j} = \sum_{\ell=j'-j}^{j'} \sum_{k=1}^{K} k\delta_{i\ell k}$, il est donc possible de traduire les variables d en variables δ de la formulation de Lorentzen et Nilsen. Par souci de clarté, nous utiliserons la notation avec les variables d.

Avec cette notation, les contraintes (3.5) de la formulation revisée de Lorentzen

et Nilsen peuvent être réécrites comme suit :

$$z \geq d^i_{J0} = \sum_{k=1}^{J} d^i_{k,k-1} \qquad \forall i. \tag{3.11}$$

Pour un certain i, $1 \leq i \leq I$, on a $z = d^i_{J0}$. Comme $\{d^i_{J0} \mid 1 \leq i \leq I\}$ sont tous des entiers naturels distincts et que z est le maximum de cet ensemble, on peut appliquer le lemme 3.24. Les contraintes (3.11) sont alors remplacées par la contrainte suivante :

$$z \geq \frac{1}{I} \sum_{i=1}^{I} d^i_{J0} + \frac{(I-1)}{2}. \tag{3.12}$$

Ce changement a pour effet d'améliorer la borne inférieure sur z de $(I-1)/2$. Il est possible de faire encore mieux. En effet, la contrainte (3.12) appartient à une famille de contraintes pour z, chacune correspondant à un sous-ensemble T des $IJ(J-1)/2$ différences d'un (I,J)-DTS. Lorsque $T = \{d^i_{J0} \mid 1 \leq i \leq I\}$ on obtient la contrainte (3.12). En général, on a

$$z \geq \frac{1}{|T|} \sum_{d^i_{j'j} \in T} d^i_{j'j} + \frac{(|T|-1)}{2}. \tag{3.13}$$

Lors de l'implémentation, on calcule les différences $d^i_{j'j}$ et on vérifie que les contraintes (3.13) ne sont pas violées pour les ensembles T consistués des n plus grandes différences, $1 \leq n \leq IJ(J-1)/2$.

Remarque 3.25. *La formulation révisée et les contraintes (3.13) assurent que la valeur de z, est toujours au moins égale à la borne inférieure triviale $M(I,J) \geq IJ(J-1)/2$, ce qui n'est pas le cas pour les formulations de Lorentzen et Nilsen.*

Les bornes inférieures pour $M(I,J)$ obtenues avec les nouvelles contraintes de Shearer sont présentées à la table 3.2.

TABLEAU 3.2 – Bornes inférieures PNE pour $M(I, J)$ (Shearer).

J	$I = 1$	$I = 2$	$I = 3$	$I = 4$	$I = 5$
1	1	2	3	4	5
2	3	6	9	12	15
3	6	12	18	24	30
4	10	20	30	40	50
5	17	32	47	62	77
6	24	46	69	91	113
7	32	63	94	124	155
8	43	83	124	164	205
9	54	106	158	209	261
10	67	132	197	261	326
11	82	161	240	320	399
12	98	194	289	385	480
13	116	229	343	456	569
14	136	268	401	534	667
15	157	311	464	618	772
16	180	356	533	709	886
17	204	405	606	807	1007
18	230	457	684	910	1137
19	258	512	767	1021	1276
20	287	571	855	1139	1422

3.4 Approche génération de colonnes

Décrivons maintenant le problème de la construction d'un (I, J)-DTS sous la forme d'un problème de génération de colonnes.

3.4.1 Formulation du problème

Premièrement, notons qu'une règle de Golomb sera simplement représentée par l'ensemble des différences qu'elle génère. Ainsi, les variables d_k du problème auxiliaire seront définies comme suit :

$$d_k = \begin{cases} 1, \text{ si } k \text{ est une différence générée par la règle,} \\ 0, \text{ sinon.} \end{cases}$$

Si t est un vecteur de différences représentant une règle de Golomb, alors dans le problème maître ces différences seront notées d_k^t.

Dans le problème auxiliaire, on considère

$$P = \{(j, j') \mid 1 \leq j < j' \leq J \text{ et } j, j' \in \mathbb{N}\}.$$

La j-ième marque d'une règle est notée m_j. Si la règle est notée t, alors dans le problème maître, nous noterons m_J^t la marque maximale de cette règle. Les variables $\delta_{jj'k}$, pour $(j, j') \in P$ seront définies comme suit :

$$\delta_{jj'k} = \begin{cases} 1, \text{ si } m_{j'} - m_j = k, \\ 0, \text{ sinon.} \end{cases}$$

Notons que les variables d_k qui apparaissent dans les contraintes du problème auxiliaire sont superflues puisqu'elles s'expriment facilement en termes des variables $\delta_{jj'k}$ et qu'elles ne servent qu'à faire le lien avec le problème maître. Pour ces mêmes contraintes, et dans ce qui suit, la constante K sera simplement une borne supérieure sur la longueur du DTS à construire.

Les autres contraintes du problème auxiliaire sont des formes équivalentes des contraintes de la formulation de Lorentzen et Nilsen (1991) présentée à la section 3.3.1.

Notons que les contraintes du problème auxiliaire ne servent en fait qu'à vérifier que l'ensemble d'entiers construit correspond bien aux différences générées par une règle de Golomb.

Dans le problème maître, on considère

$$\mathcal{T} = \{\mathcal{T}_1, \mathcal{T}_2, ..., \mathcal{T}_I\},$$

$\mathcal{T}_i$ étant l'ensemble des règles de Golomb possibles pour la i-ième règle du (I, J)-DTS. On définit alors

$$y_i^t = \begin{cases} 1, \text{ si } t \text{ est la } i\text{-ième règle du DTS.} \\ 0, \text{ sinon.} \end{cases}$$

Remarque 3.26. *Il existe deux types de symétrie pour le problème du DTS. Premièrement, la symétrie dans chacune des règles de Golomb. Dans notre formulation du problème, il n'est pas nécessaire de prendre en compte et donc d'éliminer ce type de symétrie puisque une règle de Golomb et sa règle symétrique génère le même ensemble de différences. Le deuxième type de symétrie à considérer intervient entre les J règles. Peu importe l'ordre des règles de Golomb choisies dans le DTS, tous les DTS formés de ces règles sont équivalents. Il existe plusieurs possibilités pour traiter cette symétrie. Dans notre formulation les contraintes (3.14) et (3.15) obligent les règles à être ordonnées selon l'ordre de leur élément maximal, ce qui permet d'éviter la redondance des DTS équivalents.*

Pour les coefficients de la fonction objectif du problème auxiliaire, les coefficients u_i^1, $i = 1, 2, ..., I-1$ sont les variables duales des contraintes (3.14) et u_I^1 la variable duale de la contrainte (3.15). Les coefficients u_k^2, $k = 1, 2, ..., K$, sont les variables duales des contraintes (3.16) et les coefficients u_i^3, $i = 1, 2, ..., I$ les variables duales des contraintes (3.17). Pour écrire un seul problème auxiliaire, valide pour tous les triangles, nous adopterons la convention $u_0^1 = 0$ puisque u_0^1 n'est pas définie. Les variables duales sont calculées à chaque itération à partir de la résolution de la relaxation linéaire du problème maître.

Formulation génération de colonnes (PGC)

Problème Maître

Minimisez z sous les contraintes :

$$\sum_{t\in\mathcal{T}_{i+1}} m_J^t y_{i+1}^t - \sum_{t\in\mathcal{T}_i} m_J^t y_i^t \geq 1, \qquad i = 1,2,...,I-1; \tag{3.14}$$

$$z - \sum_{t\in\mathcal{T}_I} m_J^t y_I^t \geq 0; \tag{3.15}$$

$$\sum_{i=1}^{I}\sum_{t\in\mathcal{T}_i} d_k^t y_i^t \leq 1, \qquad k = 1,2,...,K; \tag{3.16}$$

$$\sum_{t\in\mathcal{T}_i} y_i^t = 1, \qquad i = 1,2,...,I; \tag{3.17}$$

$$y_i^t \in \{0,1\}.$$

Problème Auxiliaire (pour le triangle $\mathcal{T}_i$)

Minimisez $(u_i^1 - u_{i-1}^1)m_J - \sum_{k=1}^{K} u_k^2 d_k - u_i^3$ sous les contraintes :

$$d_k \leq 1, \qquad k = 1,2,...,K; \tag{3.18}$$

$$d_k = \sum_{(j,j')\in P} \delta_{jj'k}, \qquad k = 1,2,...,K; \tag{3.19}$$

$$m_{j'} - m_j = \sum_{k=1}^{K} k\delta_{jj'k}, \qquad (j,j') \in P; \tag{3.20}$$

$$\sum_{k=1}^{K} \delta_{jj'k} = 1, \qquad (j,j') \in P; \tag{3.21}$$

$$m_0 = 0;$$

$$\delta_{jj'k} \in \{0,1\}.$$

L'implémentation de ce modèle a été faite à l'aide du logiciel Cplex au niveau des problèmes maître et auxiliaire. Comme nous nous intéressons particulièrement aux bornes inférieures sur les longueurs des DTS, le problème auxiliaire a été résolu

de manière exacte avec Cplex pour tout les résultats que nous présenterons dans la section 3.4.3. Toutefois, il est à noter qu'il serait peut-être avantageux dans le cas où le but serait la résolution exacte du problème du DTS de déterminer des heuristiques pour générer les colonnes (règles de Golomb) entrantes dans le problème maître.

Bien que la résolution exacte du problème maître n'ait pas été notre objectif principal, nous avons tout de même effectué la résolution exacte dans le cas des petits DTS, c'est-à-dire jusqu'à l'ordre des $(4, 4)$-DTS et nous avons obtenu les résultats optimaux.

Dans la section suivante nous discutons des différentes techniques de branchement qu'il serait possible d'utiliser pour la résolution exacte du problème du DTS. La méthode que nous avons utilisée dans notre implémentation, correspond au second type de branchement qui n'est peut-être pas le plus efficace au niveau du temps de calcul mais qui est certainement un des plus simple à implémenter.

3.4.2 Branchements

Pour résoudre de manière exacte le problème du DTS avec notre modèle de génération de colonnes, il faut déterminer une méthode de branchement. Le temps de résolution du problème du DTS dépend grandement de la méthode de branchement utilisée. Dans ce qui suit nous suggérons quelques méthodes de branchement qui peuvent être implémentées avec notre modèle. Il est important, dans ce qui suit, d'établir une distinction entre un triangle d'un DTS et une règle de Golomb appartenant à un DTS. Mentionnons tout d'abord qu'à strictement parler il n'y a pas de distinction entre ces deux concepts puisqu'un (I, J)-DTS est un ensemble de I règles de Golomb. Toutefois, puisque dans notre méthode de résolution nous considérons la relaxation linéaire du problème maître, une solution, pour un triangle de différences, peut alors être une combinaison linéaire de plusieurs règles de Golomb, d'où l'importance de distinguer les concepts de triangle et de règle de Golomb.

Branchement du type I

Ce type de branchement consiste simplement à fixer successivement la plus petite différence disponible tant que cela est possible, sinon on recule et on fixe une différence supérieure. Après avoir fixé qu'une différence k appartenait au triangle $\mathcal{T}_r$, si le problème auxiliaire doit être résolu pour le triangle $\mathcal{T}_r$ alors on ajoute au problème auxiliaire la contrainte

$$\sum_{(j,j')\in P} \delta_{jj'k} = d_k = 1,$$

si le triangle en question n'est pas $\mathcal{T}_r$ alors la contrainte ajoutée sera plutôt

$$\sum_{(j,j)\in P} \delta_{jj'k} = d_k = 0.$$

Deux approches sont possibles pour ce type de branchement. Premièrement, les différences peuvent être fixées sur un triangle différent à chaque fois, en conservant le nombre de différences fixées pour chaque triangle distant d'au plus 1. Deuxièmement, on peut également choisir de fixer toutes les différences d'un même triangle, puis recommencer pour le triangle suivant. On pourrait également décider de fixer un nombre quelconque de différences pour chaque triangle, toutefois de cette manière l'exhaustivité de la recherche (du parcours) serait plus difficile à démontrer.

Supposons que l'on cherche un (I, J)-DTS optimal. Le problème consiste alors, en supposant que les triangles soient ordonnées selon leurs longueurs, à déterminer I règles de Golomb d'ordre $J + 1$ disjointes avec la longueur de la I-ième règle aussi petite que possible. La condition pour couper des noeuds dans notre branchement dépend donc en grande partie de l'estimation de la longueur du I-ième triangle. Puisqu'une bonne technique de branchement en est une qui permet de couper plusieurs noeuds, il est important de voir l'effet qu'aura la fixation d'une différence dans un des triangles.

Pour considérer l'effet de l'ajout d'une différence, le rapport entre les paramètres I et J du (I, J)-DTS est important. Nous considérerons le cas où J est grand et I est petit et le cas où J est petit et I est grand. Remarquons tout d'abord qu'au fur et à mesure que le nombre de différences fixées augmente dans une règle de Golomb, il devient plus facile d'estimer la longueur qu'aura cette règle. Notons également que de manière empirique, les longueurs des règles dans un DTS sont très près l'une de l'autre. Pour cette raison, lorsque le nombre de triangles est petit la connaissance d'une des règles du DTS nous permet une bonne évaluation de la longueur du DTS.

Ainsi, dans le premier cas à considérer, le fait de connaitre les différences d'un triangle entier donne beaucoup d'information sur la longueur qu'auront les $I - 1$ autres triangles et un branchement avec les différences dans un même triangle sera privilégié. Dans le second cas, la connaissance de quelques différences pour chacun des triangles donne plus d'information sur la longueur de la I-ième règle que la connaissance entière des longueurs de quelques triangles, le branchement consistant à fixer une différence dans chaque triangle à la fois sera donc privilégié.

Remarque 3.27. *La méthode de branchement de type I permet de traiter le problème de la symétrie dans les règles de Golomb sans effort supplémentaire. En effet, comme deux règles de Golomb symétriques génèrent les mêmes différences et que le branchement de type I s'applique justement aux différences, le problème de la symétrie dans les règles de Golomb est donc inexistant.*

Remarque 3.28. *L'exhaustivité de ce type de branchement est assuré par le fait que le problème auxiliaire fournisse toujours une solution entière, c'est-à-dire une règle de Golomb. En effet, il est clair que si l'ensemble des différences est fixé pour chaque triangle alors les différences de chacun de ces triangles correspondent aux différences d'une règle de Golomb. Pour se convaincre de l'exhaustivité du branchement, il est alors suffisant de remarquer que les dernières branches consistent exactement en une partition d'un ensemble de $IJ(J-1)/2$ entiers en I classes de cardinalité $J(J-1)/2$ chacunes.*

L'illustration du branchement de type I nous permet de voir que ce branchement est déséquilibré, ce qui constitue le principal défaut de ce branchement.

$$\exists k \in \{1, 2, \ldots, K\}, \exists r \in \{1, 2, \ldots, I\} \begin{array}{l} \nearrow \; k \in \mathcal{T}_r \\ \searrow \; k \notin \mathcal{T}_r. \end{array}$$

Les contraintes obtenues de ce branchement possèdent différents niveaux de restriction. En effet, alors que la contrainte $k \notin T_r$ n'est pas très restrictive, la contrainte $k \in T_r$ est très restrictive. Ceci a pour effet de créer un branchement déséquilibré, c'est-à-dire dont la partition induite par les contraintes de l'ensemble solution possède une classe de grande cardinalité et une de petite cardinalité.

Branchement du type II

Dans ce type de branchement, qui est une forme plus restrictive du branchement de type I, en plus de spécifier à quel triangle $\mathcal{T}_r$, la différence k appartient, on demande également que cette différence soit située entre les marques j et j', pour $(j, j') \in P$. La contrainte qui doit être ajoutée au problème auxiliaire, si celui-ci fait intervenir le triangle $\mathcal{T}_r$, est alors :

$$\delta_{jj'k} = 1,$$

si le triangle en question n'est pas $\mathcal{T}_r$, alors la contrainte ajoutée sera plutôt :

$$\sum_{(j,j') \in P} \delta_{jj'k} = 0.$$

Ce branchement forme une partition de l'ensemble des solutions selon les critères suivants, en tenant compte que le branchement est toujours relatif à un triangle

donné, disons $\mathcal{T}_r$:

$$\exists k \in \{1, 2, \ldots, K\}, \exists (j, j') \in P \quad \begin{array}{l} \nearrow \quad \delta_{jj'k} = 1,\ k \in \mathcal{T}_r \\ \searrow \quad \delta_{jj'k} = 0,\ k \notin \mathcal{T}_r. \end{array}$$

L'exhaustivité de ce type de branchement est évidente puisqu'il s'agit d'un cas particulier de celui du type I. De plus, même sans résoudre le problème de génération de colonnes ce branchement trouve une solution optimale au problème du DTS. Autrement dit, ce branchement constitue une méthode exacte de résolution pour le problème du DTS.

Puisque les contraintes sont plus restrictives pour le branchement de type II, on obtient donc un branchement encore moins équilibré que celui de type I. Toutefois le fait de spécifier entre quelles marques une différence doit apparaître nous permet de ne tenir compte que des marques dans le processus de branchement, le reste des différences étant de toute manière déterminé dans le problème auxiliaire. Ceci nous permet de réduire le nombre de différences à considérer et donc le nombre de branches à explorer.

Contrairement au branchement de type I, dans le type II il faut tenir compte de la symétrie dans les règles de Golomb. En effet, comme les différences doivent être fixées entre deux marques données, et que l'effet de symétrie dans les règles de Golomb se situe justement au niveau de la position des différences dans une règle, pour éviter toute redondance due à la symétrie, il faut donc ajouter certaines contraintes supplémentaires. Ce problème est en fait très simple à résoudre, il suffit par exemple d'ajouter dans le problème auxiliaire une contrainte stipulant que la différence entre les deux dernières marques doit être supérieure à la différence entre les deux premières.

Branchement du type III (Ryan-Foster)

Pour obtenir un branchement mieux équilibré que le branchement de type I, il est possible de conserver le principe de branchement sur les différences en utilisant un branchement du type Ryan-Foster. Dans ce branchement, la restriction des contraintes fournies par le branchement est modifiée par le fait qu'on ne spécifie pas directement si une différence appartient ou non au DTS. L'idée est simplement de créer une relation pour l'appartenance des différences au DTS. Pour illustrer cette idée, voici l'expression du branchement :

$$\exists k, k' \in \{1, 2, \ldots, K\} \begin{cases} \nearrow & d_k \text{ et } d_{k'} \text{ apparaissent dans le DTS ou} \\ & d_k \text{ et } d_{k'} \text{ n'apparaissent pas dans le DTS} \\ \searrow & \text{exactement une différence parmi } d_k \text{ et } d_{k'} \\ & \text{apparaît dans le DTS.} \end{cases}$$

Les classes issues de la partition induite par le branchement contiennent d'une part les solutions dont k et k' font soient toutes deux parties du DTS ou en sont toutes les deux absentes, et d'autre part les solutions où une seule des différences k ou k' fait partie du DTS. Ces contraintes doivent être ajoutées au problème maître puisqu'elle ne fournissent aucune information à savoir si une différence appartient ou non au DTS. Une fois que les différences appartenant au DTS sont fixées par les branchements, il est également possible d'utiliser le même type de branchement pour déterminer à quel triangle les différences appartiennent.

Bien que ce type de branchement ait l'avantage d'être mieux équilibré que celui de type I, il demeure toujours un inconvénient avec ce type de branchement. En effet, puisque les contraintes ajoutées se rapportent uniquement à deux différences et que les différences qui doivent apparaître dans une solution optimale du DTS sont inconnues, il est possible que beaucoup de branchements doivent être effectués avant de déterminer quelles sont les différences appartenant au DTS, ce qui équivaut à une perte de temps pour la résolution du problème.

L'exhaustivité de ce type de branchement est assuré en considérant, d'une part, toutes les paires de différences parmis toutes les différences possibles, c'est-à-dire les entiers $1, 2, \ldots, K$, puis d'autre part, les paires de différences parmi les sous-ensembles formant possiblement un triangle du DTS. Encore une fois ceci montre l'ampleur du nombre de branchements qu'il peut être nécessaire de faire pour obtenir une solution optimale. Il faut également noter que certaines observations ou certains cas particuliers peuvent permettre de réduire le nombre de branches à explorer, c'est-à-dire le nombre de paires de différences à considérer. Par exemple, deux différences k et k' telles que $k+k' > K$ implique que ces deux différences ne peuvent pas appartenir au même triangle. Il semble toutefois que le nombre de ces réductions soit limité par rapport aux paires à considérer, ce qui laisse toujours place à amélioration en matière de branchement.

Branchement du type IV (Vanderbeck)

Pour obtenir une méthode de branchement efficace, il est essentiel de trouver un critère de branchement qui partitionne l'espace des solutions de manière équilibrée. Dans cette partie, nous adaptons une méthode générale de branchement présentée par Vanderbeck (2000) qui offre cet avantage. Cette méthode peut être adaptée sans trop de difficulté à notre modèle pour résoudre le problème du DTS. Les techniques de branchement que nous avons explorées jusqu'ici agissaient uniquement sur une ou deux variables à la fois, il apparaît que ces techniques donnent généralement des branchements non équilibrés, c'est-à-dire telles que la partition de l'ensemble des solutions possibles contiennent une classe de grande cardinalité et une classe de petite cardinalité. L'idée de la méthode de Vanderbeck est de brancher sur un ensemble de variables afin d'obtenir un branchement le plus équilibré possible.

Après avoir résolu la relaxation linéaire du problème maître, si la solution obtenue n'est pas entière, ce qui est généralement le cas, alors les deux cas suivants sont possibles :

(1) il existe un indice $i, 1 \leq i \leq I$ tel que $\sum_{k \in K} \sum_{t \in \mathcal{T}_i} kd_k^t y_i^t = \alpha_i$ est fractionnaire, c'est-à-dire que la somme de toutes les marques appartenant au i-ième triangle du DTS est fractionnaire,

(2) il existe deux règles t et t' appartenant au même triangle $\mathcal{T}_i$ avec au moins une marque qui n'est pas la même, c'est-à-dire qu'il existe un indice $j, 0 < i \leq J$ tel que $m_j^t \neq m_j^{t'}$.

Notons que le premier critère de branchement prévaut toujours sur le second. Autrement dit, tant que la valeur de α_i n'est pas entière, le critère (1) est appliqué. La raison de ce choix, comme nous l'avons déjà mentionné, est qu'en effectuant le branchement sur plusieurs variables à la fois cela donne un branchement plus équilibré comparé au branchement effectué sur une seule variable. Toutefois, puisqu'il est possible que α_i soit un entier pour tous les triangles $\mathcal{T}_i$ et que la solution au problème du DTS reste fractionnaire, dans ce cas il faut alors se résoudre à brancher sur une seule variable à la fois, donc à utiliser le critère (2).

Dans le premier cas où la valeur de α_i est fractionnaire, le critère de branchement (1) s'exprime comme suit :

$$\sum_{k \in K} \sum_{t \in \mathcal{T}_i} kd_k^t y_i^t = \alpha_i \quad \begin{array}{l} \nearrow \ \sum_{k \in K} \sum_{t \in \mathcal{T}_i} kd_k^t y_i^t \leq \lfloor \alpha_i \rfloor \\ \\ \searrow \ \sum_{k \in K} \sum_{t \in \mathcal{T}_i} kd_k^t y_i^t \geq \lceil \alpha_i \rceil. \end{array} \qquad (1)$$

Ces contraintes sont alors ajoutées au problème maître, générant ainsi deux nouvelles branches à explorer.

Dans le second cas où la valeur de α_i est entière et que nous devons brancher sur une seule variable, correspondant à une marque d'un triangle, le critère de branche-

ment (2) s'exprime comme suit :

$$\exists t, t' \in \mathcal{T}_i : m_j^t \neq m_j^{t'} \quad \begin{array}{l} \nearrow \\ \\ \searrow \end{array} \quad \begin{array}{l} m_j \leq \frac{\sum_{t \in \mathcal{T}_i} m_j^t}{|\mathcal{T}_i|} - 1 \\ \\ m_j \geq \frac{\sum_{t \in \mathcal{T}_i} m_j^t}{|\mathcal{T}_i|} \ . \end{array} \qquad (2)$$

Ces contraintes sont alors ajoutées au problème auxiliaire relatif au triangle $\mathcal{T}_i$, générant encore deux nouvelles branches. Il est important de noter que bien qu'il ne soit pas nécessaire d'ajouter ces contraintes au problème maître, il faut supprimer les règles qui apparaissent déjà dans le problème maître et qui ne satisfont pas ces contraintes. Par la suite, lorsque les règles entrantes seront générées par le problème auxiliaire, elles satisferont nécessairement ces contraintes.

Les détails du branchement de type IV, c'est-à-dire les conditions sous lesquelles les branches doivent être élaguées pour que le branchement fonctionne, sont donnés dans la preuve de notre proposition suivante.

Proposition 3.29. *Ce branchement est exhaustif et nous fournit une solution optimale au problème du DTS.*

Preuve. Supposons que nous cherchions un (I, J)-DTS optimal. Nous savons qu'il existe une borne supérieure sur la longueur du (I, J)-DTS optimal, à savoir, la longueur du meilleur (I, J)-DTS connu, que nous avons noté K jusqu'ici. Ceci nous donne donc une borne supérieure pour la valeur de α_i pour tous les triangles $\mathcal{T}_i$ possibles. En effet, puisque toutes les différences d'un triangle doivent être distinctes et que le nombre de différences est $J(J+1)/2$ alors une borne supérieure est donnée par

$$\sum_{i=0}^{J(J+1)/2-1} K - i.$$

Par un raisonnement analogue, on obtient

$$\sum_{i=1}^{J(J+1)/2} i$$

comme borne inférieure de α_i pour tous les triangles $\mathcal{T}_i$.

Puisque toutes les valeurs des α_i dans les contraintes issues du critère (1) sont bornées inférieurement et supérieurement, il suffit donc de montrer que le branchement est exhaustif pour démontrer qu'une solution optimale sera toujours fournie. Pour démontrer l'exhaustivité du branchement, regardons sous quelles conditions il est permis de couper une branche.

Considérons tout d'abord le critère (1). Pour qu'une branche soit éliminée les conditions possibles sont, d'une part, qu'une borne inférieure ou supérieure sur les sommes des différences pour un triangle $\mathcal{T}_i$ soit atteinte, c'est-à-dire pour les valeurs de $\lfloor \alpha_i \rfloor$ ou de $\lceil \alpha_i \rceil$ dépasse une borne ou d'autre part, que pour toute solution possible de la relaxation du problème maître, la meilleure borne supérieure sur la longueur du DTS soit atteinte. Dans le premier cas, la coupure du branchement correspond uniquement à des parties à l'extérieur de l'ensemble des solutions possibles. Dans le second cas, les coupures correspondent à des parties de l'ensemble solution ne pouvant fournir au mieux qu'une valeur égale à la meilleur solution entière connue pour le (I, J)-DTS, c'est-à-dire la borne supérieure courante du (I, J)-DTS. Puisque dans tous les cas, aucune solution optimale ne peut être exclue par le critère (1) du branchement, il ne reste plus, pour démontrer la proposition, qu'à montrer qu'aucune solution de longueur moindre que la borne supérieure courante du (I, J)-DTS ne peut être exclue par le critère (2).

Fixons tout d'abord qu'une branche doive être éliminée pour le critère (2) si et seulement si la relaxation linéaire du problème maître donne une solution dont la valeur plafond est supérieure ou égale à la borne supérieure courante du (I, J)-DTS. Soient $R_1, R_2, \ldots, R_I$, des règles de Golomb formant un (I, J)-DTS de longueur

moindre que la borne supérieure courante et satisfaisant les contraintes induites jusqu'ici par les critère (1) et (2). De plus, supposons que la somme des différences soit entière pour tous les triangles, sinon le critère (1) doit être appliqué. Regardons ce qui arrive alors en appliquant le critère (2) du branchement pour un triangle particulier, disons $\mathcal{T}_i$, et pour une marque donnée, disons m_j. Rappelons que pour le critère (2) les contraintes sont ajoutées au problème auxiliaire. Ainsi dans une des branches la contrainte ajoutée sera $m_j \leq n-1$ et dans l'autre branche la contrainte ajoutée sera $m_j \geq n$. Donc au moins une des branches permettra la solution $R_1, R_2, \ldots, R_I$, or la solution de la relaxation linéaire du problème maître est bornée supérieurement par la longueur de R_I. Il est donc impossible que la branche permettant la solution $R_1, R_2, \ldots, R_I$ soit éliminée à cause du critère (2). Ceci étant vrai pour toute solution de longueur moindre que la borne supérieure courante du (I, J)-DTS, la démonstration de l'exhaustivité du branchement est terminée.

Donc le branchement de type IV est exhaustif et nous fournit toujours une solution optimale au problème du DTS.

□

3.4.3 Propriétés du modèle PGC et bornes inférieures

La proposition suivante sert à valider notre modèle en démontrant l'équivalence de la solution entière obtenue par notre modèle et de celle obtenue par le modèle de Lorentzen et Nilsen.

Proposition 3.30. *La formulation génération de colonnes (PGC) est équivalente à la formulation en nombres entiers (PNE) de Lorentzen et Nilsen.*

Preuve. Notons tout d'abord que les contraintes du problème auxiliaire de PGC sont équivalentes aux contraintes du PNE lorsque $I = 1$. En effet, les contraintes (3.20)

sont les mêmes que les contraintes (3.2), les contraintes (3.21) sont les mêmes que les contraintes (3.3) et les contraintes (3.18) et (3.19) sont les mêmes que les contraintes (3.4). Ainsi, chaque solution du problème auxiliaire correspond bien à une règle de Golomb. Autrement dit, chaque vecteur t de PGC correspond à une règle de Golomb.

Pour montrer que les deux formulations sont équivalentes, nous montrerons qu'une solution de PNE est équivalente à une solution de PGC et que toute solution de PGC est une solution de PNE.

Soit $\Delta = \{\Delta_1, \Delta_2, ..., \Delta_I\}$ une solution obtenue de PNE. Il se peut qu'il existe i et i' tels que $1 \leq i < i' \leq I$ et $m_{iJ} > m_{i'J}$. Toutefois, comme nous l'avons déjà mentionné, il est possible de permuter les indices des Δ_i pour que les éléments maximaux de chaque règle soient ordonnés de façon croissante, obtenant ainsi une solution équivalente. Supposons donc sans perte de généralité que les éléments maximaux de la solution Δ soient ordonnés de manière croissante. Puisque les m_{iJ} sont des entiers distincts et que $m_{i'J} > m_{iJ}$ implique $i' > i$ alors les contraintes (3.14) et (3.15) sont satisfaites.

Les contraintes (3.17), qui imposent que pour chaque indice i il y ait une règle de Golomb t correspondante, sont nécéssairement satisfaites pour la solution Δ.

Les contraintes (3.16), qui imposent que chaque différence k apparaisse au plus une fois dans les différences générées par le DTS, sont exactement les mêmes que les contraintes (3.4).

Ainsi, pour toute solution de PNE il existe une solution équivalente satisfaisant toutes les contraintes de PGC.

Inversement, soit $\Delta = \{\Delta_1, \Delta_2, ..., \Delta_I\}$ une solution obtenue de PGC. Comme nous venons de le dire, les contraintes (3.4) sont équivalentes aux contraintes (3.16), elles doivent donc être satisfaites par la solution Δ.

Les contraintes (3.2) et (3.3) imposent que chaque différence entre deux marques soit fixée et unique. Que chaque différence soit fixée est imposée par le problème auxiliaire et les contraintes (3.17), qu'elle soit unique est imposée par les contraintes (3.16). Les contraintes (3.2) et (3.3) doivent donc être satisfaites par la solution Δ.

Les contraintes (3.14) et (3.15) impliquent que les contraintes (3.1) doivent être satisfaites.

Ainsi, pour toute solution de PGC, toutes les contraintes de PNE sont satisfaites et on a bien une solution de PNE.

Puisque les objectifs des deux formulations sont les mêmes et que les ensembles de solutions des deux formulations sont équivalents, alors les deux formulations sont bien équivalentes.

□

La proposition précédente nous indique que la solution optimale de notre modèle est équivalente à la solution optimale du modèle de Lorentzen et Nilsen. Toutefois, si l'on s'intéresse à la borne inférieure obtenue par la résolution de la relaxation linéaire de notre modèle, nous pouvons constater que notre modèle donne une meilleure borne inférieure que celui de Lorentzen et Nilsen. Ce fait est exprimé dans la proposition suivante.

Proposition 3.31. *La borne inférieure obtenue de la relaxation linéaire de la formulation génération de colonnes (PGC) est supérieure ou égale à celle obtenue de la formulation en nombres entiers (PNE) de Lorentzen et Nilsen.*

Preuve. Pour établir cette démonstration, il faut montrer que toutes les contraintes de la relaxation linéaire de la formulation (PNE) sont satisfaites par les contraintes

de la relaxation linéaire de la formulation (PGC). Notons d'abord que les contraintes (3.2) du PNE sont assurées d'être satisfaites par toutes règles de Golomb générées par le problème auxiliaire, c'est-à-dire par toutes les colonnes entrantes dans le problème maître. En effet, il suffit de remarquer que les contraintes (3.20) du problème auxiliaire sont exactement les mêmes.

La satisfaction des contraintes (3.3) du PNE est assurée par les contraintes (3.17) du PGC. En effet, les contraintes (3.3) stipulent que pour chaque paire de marques dans un même triangle, le nombre de différences (avec possiblement des coefficients fractionnaires) entre ces marques est exactement un alors que les contraintes (3.17) stipulent que dans chaque triangles le nombre de règles de Golomb (avec possiblement des coefficients fractionnaires) est exactement un. Les deux affirmations sont équivalentes puisque dans une règle de Golomb le nombre de différences entre chaque paire de marques est exactement un. Les contraintes (3.3) du PNE sont donc équivalentes aux contraintes (3.17) du PGC.

Les contraintes (3.4) du PNE et les contraintes (3.16) du PGC stipulent, dans leur formulation respective, que chaque différence k, $1 \leq k \leq K$, doit être choisie au plus une fois, elles sont évidemment équvalentes.

Il ne reste donc qu'à considérer les contraintes (3.1) du PNE. Ces contraintes sont certainement respectées par toute solution de la relaxation de PGC. En effet, les contraintes (3.14) et (3.15) impliquent que la variable z, correspondant à la longueur du DTS, doit être supérieure ou égale à la longueur de tous les triangles, ce qui correspond aux contraintes (3.1) du PNE.

□

La résolution de la relaxation linéaire du problème maître nous donne les résultats du Tableau 3.3 comme bornes inférieures sur les valeurs de $M(I, J)$.

TABLEAU 3.3 – Bornes inférieures pour génération de colonnes.

	Bornes Inférieures sur z				
J	$I=1$	$I=2$	$I=3$	$I=4$	$I=5$
1	1	2	(3)	(4)	(5)
2	3	5.75	(8.5)	(11.25)	(14)
3	6	(11.52)	(17)	(22.5)	(28)
4	11	20	(29.5)	(39)	(48.5)
5	17	(31.1667)	(46.1667)	(61.1667)	(76.1667)

Remarque 3.32. *La proposition 3.31 stipule que notre modèle donne une borne inférieure de qualité supérieure ou égale à celle obtenue du modèle PNE de Lorentzen et Nilsen. Pour démontrer la proposition, nous avons simplement montré que la borne de notre modèle est au moins égale à celle de PNE. Toutefois on peut remarquer en comparant les Tableaux 3.1 et 3.3 que la borne obtenue de notre modèle est strictement supérieure à celle de Lorentzen et Nilsen dans la plupart des cas. Les valeurs entre parenthèses dans le Tableau 3.3 améliorent la borne inférieure de Lorentzen et Nilsen.*

Comme pour le modèle de Lorentzen et Nilsen, il est possible avec notre modèle d'obtenir une borne inférieure $M(I,J)$ de moins bonne qualité que la borne inférieure triviale, c'est-à-dire $IJ(J+1)/2$. Cette affirmation peut être vérifiée en regardant les valeurs du Tableau 3.3. Toutefois, avec des modifications mineures apportées à notre modèle, il est possible de pourvoir à ce problème. L'idée, consiste simplement à ajouter les coupes équivalentes à celles que Shearer a ajouté au modèle de Lorentzen et Nilsen pour améliorer leurs bornes inférieures. Nous présentons dans ce qui suit, les modifications nécessaires à cette fin.

Rappelons que les coupes de Shearer que nous avons présentées à la section 3.3.3 s'expriment comme suit, sous la forme générale, pour tout sous-ensemble de différences S du (I,J)-DTS :

$$z \geq \frac{1}{|S|} \sum_{d^i_{j'j} \in S} d^i_{j'j} + \frac{(|S|-1)}{2} \qquad (1)$$

où $d^i_{j'j}$ désigne la différence entre les marques j' et j dans le triangle $\mathcal{T}_i$.

Modifications du problème maître

Pour tenir compte des différences entre les marques, des variables correspondantes aux marques doivent être ajoutées aux problème maître du modèle PGC. Notons m_{ij} ces nouvelles variables. Les marques elles-mêmes doivent également être ajoutées aux colonnes du problème maître, notons m^t_j la j-ième marque de la colonne t, pour $t \in \mathcal{T}_i$. Les contraintes à ajouter au problème maître sont alors :

$$m_{ij} = \sum_{t \in \mathcal{T}_i} y_t m^t_j, \qquad j = 0, 1, \ldots, J, \;\; i = 1, 2, \ldots, I \qquad (2)$$

Génération des coupes

Pour générer les contraintes (1), on résout le problème maître qui nous donne une solution optimale $\bar{\Delta} = (\bar{y}, \bar{m})$. Il suffit alors de trouver une contrainte (1) qui soit violée par cette solution ou de montrer que toutes ces contraintes sont satisfaites par la solution trouvée.

Ce problème est résolu par la procédure suivante :

1. Calculer $\bar{d}^i_{j'j} = \bar{m}_{ij'} - \bar{m}_{ij}$, pour $i = 1, 2, \ldots, I$ et $0 \leq j < j' \leq J$;
2. Ordonner les différences obtenues en 1. Soit $s(\bar{\Delta})$ le vecteur ordonné des différences. Il faut garder une trace des indices i, j et j' tel que $s_t(\bar{\Delta}) = d^i_{j'j}$: notons $(i, j, j')_t$ le triplet correspondant à $s_t(\bar{\Delta})$;
3. Pour tout $\ell = 2, 3, \ldots, \frac{IJ(J+1)}{2}$, calculer $A_\ell = \ell \bar{m}_{IJ} - \sum_{t=1}^{\ell} s_t(\bar{\Delta})$. Si $A_\ell < \frac{\ell(\ell-1)}{2}$, alors on arrête : $S = \{(i, j, j')_1, (i, j, j')_2, \ldots, (i, j, j')_\ell\}$ définit une contrainte violée ;
4. Si la procédure arrive ici, toutes les contraintes (1) sont satisfaites.

Modifications du problème auxiliaire

La fonction objectif du problème auxiliaire doit être modifiée pour tenir compte des nouvelles variables ajoutées au problème maître. Soit u_{ij}^4 la variable duale associée à la contrainte (2) avec $1 \leq i \leq I$ et $0 \leq j \leq J$. Le terme

$$\sum_{j=0}^{J} u_{ij}^4 m_j$$

doit être ajouté au coût réduit de la variable y^t pour le triangle $\mathcal{T}_i$, et par conséquent dans la fonction objectif du problème auxiliaire pour le triangle $\mathcal{T}_i$.

Puisque les variables y^t n'apparaissent pas dans les contraintes (1), les variables duales correspondantes à ces contraintes n'ont pas à être ajoutées au coût réduit des variables y^t, et par conséquent elles n'affectent en rien la fonction objectif du problème auxiliaire.

L'ajout des coupes de Shearer à notre modèle de génération de colonnes nous permet d'obtenir de meilleures bornes inférieures, mais cela n'est pas encore suffisant pour nous garantir l'obtention de la borne triviale. En effet, dans le Tableau 3.4 qui nous montre les résultats obtenus en considérant les coupes de Shearer, on peut voir que la borne inférieure obtenue pour le (5,3)-DTS est 29 alors que la borne triviale, qui correspond au nombre de différences dans le (5,3)-DTS, est 30.

Pour garantir l'obtention de la borne inférieure triviale, il suffit d'ajouter au problème maître la contrainte stipulant que la somme des $IJ(J+1)/2$ différences dans le (I,J)-DTS doit être au moins égale à la somme des $IJ(J+1)/2$ premiers entiers. Cette contrainte peut être ajoutée au problème maître sous la forme suivante :

$$\sum_{i=1}^{I} \sum_{t \in \mathcal{T}_i} \sum_{k=1}^{K} k d_k^t y_i^t \geq \frac{N(N+1)}{2}, \qquad \text{où } N = \frac{IJ(J+1)}{2}. \tag{3}$$

TABLEAU 3.4 – Bornes inférieures pour PGC avec coupes de Shearer.

	Bornes Inférieures sur z				
J	$I=1$	$I=2$	$I=3$	$I=4$	$I=5$
1	1	2	3	4	5
2	3	6	9	11.5854	14.2151
3	6	12	17.5	23.25	29
4	11	20	30	40	50
5	17	31.3333	46.5	61.6667	76.8333
6	24	45.875	68.25	90.625	113

En considérant pour les contraintes (1), l'ensemble de toutes les différences, on obtient

$$z \geq \frac{1}{|S|} \sum_{d^i_{j'j} \in S} d^i_{j'j} + \frac{(|S|-1)}{2}, \text{ où } |S| = \frac{IJ(J+1)}{2}.$$

La contrainte (3) implique que la somme de toutes les différences est au moins la somme des $IJ(J+1)/2$ premiers entiers, on obtient donc comme borne inférieure, pour $|S| = \frac{IJ(J+1)}{2}$:

$$z \geq \frac{(|S|+1)}{2} + \frac{(|S|-1)}{2} = \frac{IJ(J+1)}{2}.$$

Par conséquent, avec les coupes (1) et la contrainte (3), le modèle PGC atteint assurément la borne inférieure triviale.

Remarque 3.33. *Nous venons de voir que pour obtenir une borne inférieure de meilleure qualité, c'est-à-dire qui nous assure d'avoir au moins la borne triviale, les coupes de Shearer peuvent être ajoutées, ainsi que la contrainte (3), dans la relaxation linéaire de notre modèle PGC. Notons que dans le cas où nous voulons appliquer ces coupes pour résoudre le problème du DTS, c'est-à-dire en utilisant un branchement, il suffit simplement de considérer pour chaque branche les coupes qui peuvent être ajoutées sans tenir compte de l'endroit où l'on se situe dans le branchement. Autrement dit, les contraintes (1) et la contrainte (3) n'ont jamais à être enlevées lorsque l'on effectue un retour arrière dans un branchement puisqu'elles sont globalement valides, c'est-à-dire que n'importe quelle solution réalisable satisfera ces contraintes.*

TABLEAU 3.5 – Bornes inférieures pour PGC avec contrainte (3) et coupes de Shearer.

	Bornes Inférieures sur z				
J	$I=1$	$I=2$	$I=3$	$I=4$	$I=5$
1	1	2	3	4	5
2	3	7	10	12	15
3	6	12	18	24	30
4	11	21	31	41	51
5	17	32	48	63	79
6	24	47	69	92	116

En ajoutant la contrainte (3) dans le problème maître, il faut modifier la fonction objectif du problème auxiliaire pour tenir compte de la modification apportée aux coûts réduits. Soit u^5 la variable duale associée à la contrainte (3). Le terme

$$u^5 \sum_{k=1}^{K} k d_k^t$$

doit être ajouté au coût réduit de la variable y_i^t et par conséquent à la fonction objectif du problème auxiliaire. Les résultats obtenus en considérant les coupes de Shearer et la contrainte (3) sont présentés dans le Tableau 3.5. Ce sont les meilleures bornes inférieures obtenues par programmation linéaire.

Comme nous l'avons déjà mentionné, l'implémentation du modèle PGC a été faite à l'aide du logiciel Cplex au niveau des problèmes maître et auxiliaire. Dans l'implémentation, plutôt que de résoudre le problème auxiliaire à l'optimalité, nous choisissions la première solution dont la valeur de la fonction objectif est négative, c'est-à-dire une variable du problème maître ayant un coût réduit négatif.

La résolution de la relaxation linéaire du problème maître nous donne les bornes inférieures du Tableau 3.5. Les temps de calcul pour obtenir ces bornes sont présentés au Tableau 3.6. Ces temps tiennent évidemment compte de la génération des coupes de Shearer. Ces calcul ont été effectués sur un ordinateur muni d'un processeur de 3.40 GHz.

TABLEAU 3.6 – Temps de calcul des meilleures bornes inférieures

	Temps pour trouver z optimal			
J	$I = 2$	$I = 3$	$I = 4$	$I = 5$
2	0.24 sec	0.21 sec	0.10 sec	0.11 sec
3	0.53 sec	0.84 sec	0.15 sec	0.17 sec
4	1.03 sec	2.23 sec	8.83 sec	5.95 sec
5	8.78 sec	20.75 sec	40.29 sec	1 min 22 sec
6	6 min 52 sec	8 min 01 sec	14 min 57 sec	4 h 58 min

Remarque 3.34. *Dans le Tableau 3.6 la colonne correspondant à $I = 1$ n'apparaît pas puisque ce cas équivaut à résoudre le problème de la règle de Golomb par le modèle de Lorentzen et Nilsen. De même, la ligne correspondant à $J = 1$ est absente du tableau puisque notre modèle oblige les triangles à avoir des longueurs différentes d'au moins une unité, et de cette façon, la solution optimale est immédiatement obtenue.*

CONCLUSION

Dans cette thèse, nous nous sommes intéressés à deux problèmes combinatoires réliés au problème d'affectation de fréquences : les T-colorations et les règles de Golomb. Nous avons vus que ces deux problèmes sont non seulement reliés au problème PAF mais ont des applications considérables dans plusieurs domaines. Dans cette thèse nous nous sommes contentés de présenter ces applications uniquement pour justifier l'étude des problèmes de la T-coloration et de la règle de Golomb. Bien que ces domaines d'application représentent souvent des domaines d'un grand intérêt, par exemple le domaine du codage par rapport aux problèmes de la règle de Golomb et ses généralisations, nous avons choisi de restreindre au minimum les références à la réalité pour nous consacrer à l'aspect théorique des problèmes traités dans cette thèse.

Le premier problème traité dans cette thèse est le problème de la T-coloration. La présentation des résultats concernant les T-colorations nous montre qu'ils sont presque toujours reliés à une forme particulière de l'ensemble T. Nous nous sommes intéressés au problème de manière inverse, c'est-à-dire en cherchant à fixer des classes de graphes pour lesquelles il était possible de déterminer l'étendue optimale d'une T-coloration quel que soit l'ensemble T fourni.

Pour déterminer la T-étendue optimale des graphes nous avons fourni des algorithmes qui fonctionnent en temps polynomiaux. Nous avons fourni des algorithmes pour la classe des cycles et la classe des roues. Nous avons déterminé sous quelles conditions la T-étendue d'une subdivision de K_4 pouvait être déterminé en temps polynomial. Puis nous avons fourni sous la forme d'un algorithme polynomial une formule pour obtenir des bornes sur la T-étendue de subdivisions de roues. Finalement, en nous basant sur le concept de T-graphe nous avons déterminé un algorithme

polynomial pour obtenir une borne sur la T-étendue des graphes 3-colorables quel que soit l'ensemble T.

Pour déterminer un algorithme nous permettant d'obtenir une borne sur la T-étendue des graphes 3-colorables on utilise implicitement le fait que le problème de T-coloration d'un graphe biparti est trivial. Ceci semble rendre la tâche plus complexe pour l'obtention du même genre d'algorithme en temps polynomial pour les graphes 4-colorables, qui devraient alors considérer les graphes 3-colorables et non plus les graphes bipartis.

Le second problème abordé est le problème de la règle de Golomb. Tous les autres problèmes traités dans cette thèse sont des généralisations de ce problème. Les meilleures solutions connues au problème de la règle de Golomb sont des solutions obtenues par les méthodes algébriques. L'optimalité des règles de Golomb est connue pour les règles de Golomb jusqu'à l'ordre 25. Parmi ces règles optimales seulement quelques unes ne correspondent pas à une droite d'une géométrie projective ou semi-affine. Toutefois, en appliquant certaines réductions sur les ensembles correspondant aux droites d'une géométrie finie, on obtient pour tous les ordres inférieures ou égal à 25, une règle de Golomb de longueur optimale.

Les méthodes algébriques, correspondant à la construction de géométrie finie pour le problème de la règle de Golomb, font parties du domaine de la connaissance générale et apparaissent dans la littérature sous des formes assez disparates. Dans une première phase, nous avons présenté les justifications des différentes approches algébriques puis nous avons dans une seconde implémenté une heuristique de construction de règles de Golomb en nous basant sur ces justifications. Cette heuristique qui donne les meilleures solutions jusqu'à l'ordre 25 pour les règles de Golomb, sauf pour quelques exceptions, nous fournit des solutions jusqu'à l'ordre 500 dans des temps de quelques minutes alors que les meilleures méthodes exactes prennent en théorie plusieurs années pour des règles d'ordre environ 20. En particulier, la preuve de l'optimalité pour la règle de Golomb d'ordre 23 a nécessité plusieurs mois de calcul sur

des milliers d'ordinateurs alors qu'on obtient cette règle en moins d'une seconde avec notre heuristique.

En apportant des modifications mineures à l'heuristique de construction des règles de Golomb, nous avons obtenu un heuristique pour construire des ensembles doublement orthogonaux. Les applications des ensembles doublement orthogonaux se situent en théorie du codage. Notre heuristique ainsi construit nous a fourni, pour presque tous les ordres jusqu'à 30, les meilleurs ensembles doublement orthogonaux.

Comme pour les règles de Golomb et en général pour les méthodes algébriques notre heuristique de construction d'ensembles doublement orthogonaux a pour principal inconvénient l'impossibilité de démontrer l'optimalité des solutions obtenues. Toutefois, comme pour les règles de Golomb le temps de calcul pour notre heuristique est beaucoup plus petit que le temps de calcul des heuristiques basées sur les méthodes exactes, ce qui en pratique compense largement pour l'impossibilité de prouver l'optimalité.

Le dernier problème que nous avons considéré est le problème du DTS. Nous avons tout d'abord commencé par présenter les nombreuses approches algébriques qui ont été proposées et qui donnent les meilleures solutions connues pour le problème du DTS. Puis nous avons présenté un modèle de programmation linéaire en nombre entier, proposé par Lorentzen et Nilsen, et les différentes améliorations apportées à ce modèle. Nous avons finalement proposé un modèle basé sur le principe de génération de colonnes. L'implémentation de ce modèle nous fournit les meilleures bornes inférieures obtenues par programmation linéaire pour la longueur des DTS.

Bien que les temps de calcul deviennent important même pour les petits DTS, la recherche de bornes inférieures est importante, d'une part, parce que les bornes inférieures fournies sont bonnes pour les DTS, en comparaison avec les valeurs optimales qui sont connues, et d'autre part, parce que les meilleures valeurs connues

sont obtenues par les méthodes algébriques qui ne peuvent garantir l'optimalité des solutions fournies. Comparativement, pour le problème de la règle de Golomb les bornes inférieures sont généralement de mauvaise qualité, et donc l'effort mis dans la recherche de telles bornes s'avère la plupart du temps inutile.

À l'origine, l'idée d'utiliser le principe de la génération de colonnes pour résoudre le problème du DTS nous est venu du fait que les méthodes algébriques fournissaient très rapidement une grande quantité de règles de Golomb. Nous avons donc pensé allier les avantages des méthodes algébriques aux méthodes issues de la programmation linéaire, en utilisant les méthodes algébriques comme heuristique pour générer des colonnes entrantes, donc des règles de Golomb, dans le problème maître de notre modèle de génération de colonnes. Nous avons hélas échoué dans cette tentative de réunir les différentes approches. Mais l'idée de mettre à profit la rapidité et l'efficacité des solutions obtenues par les méthodes algébriques reste très prometteuse pour résoudre exactement le problème du DTS.

BIBLIOGRAPHIE

ATKINSON, M. D., SANTORO, N. et URRUTIA, J. (1986). Integer sets with distinct sums and differences and carrier frequency assignments for nonlinear repeaters. *IEEE Transactions on Communications.* 34:6. P. 614–617.

BABCOCK, W. C. (1953). Intermodulation interference in radio systems. *Bell Systems Technical Journal.* P. 63–73.

BERMOND, J. C. (1979). Graceful graphs, radio antennae and French windmills. *Graph Theory and Combinatorics.* 34 de *Research Notes in Mathematics.* London, UK : Pittman. P. 18–37.

BERMOND, J. C., KOTZIG, A. et TURGEON, J. M. (1976). On a combinatorial problem of antennas in radioastronomy. *Proceedings of 18th Hungarian Combinatorial Colloquia.* P. 135–149.

BLOOM, G. S. et GOLOMB, S. W. (1977). Applications of numbered complete graph. *Proceedings of the IEEE.* 65. P. 562–570.

BLOOM, G. S. et GOLOMB, S. W. (1978). Numbered complete graph, unusual rulers, and assorted applications. *Theory and Applications of Graph.* Lecture Notes in Mathematics. Springer Verlag. P. 53–65.

BOSE, R. C. (1942). An affine analogue of Singer's theorem. *J. Indust. Math. Soc..* 6. P. 1–15.

CARDINAL, C., HACCOUN, D., GAGNON, F. et BATANI, N. (1999). Turbo decoding using convolutional self doubly orthogonal codes. *ICC '99 - 1999 IEEE International Conference on Communications.* P. 113–117.

CHEN, W. (1983). Lower bound of constraint length of self-orthogonal convolutional codes. *Kexue Tongbao.* special issue. P. 75–78.

CHEN, W. et KLøVE, T. (1991). Lower bounds on multiple difference sets. *Discrete Mathematics.* 98:1. P. 9–21.

CHEN, Z. (1994). Further results on difference triangle sets. *IEEE Transactions on Information Theory.* 40:4. P. 1268–1270.

CHEN, Z., FAN, P. et JIN, F. (1992). Disjoint difference sets, difference triangle sets, and related codes. *IEEE Transactions on Information Theory.* 38:2. P. 518–522.

CHU, W. et GOLOMB, S. W. (2003). A note on equivalence between strict optical orthogonal codes and difference triangle sets. *IEEE Transactions on Information Theory.* 49:3. P. 759–761.

COOLSAET, K. n.d. *http ://www.inference.phy.cam.ac.uk/cds/.*

DAVIES, R. O. (1959). On Langford's problem (II). *Mathematical Gazette.* 43. P. 253–255.

DEWDNEY, A. K. (1985). Computer recreations. *Scientific American.* Décembre. P. 16–26.

DOLLAS, A., RANKIN, W. et McCRACKEN, D. (1998). A new algorithm for Golomb ruler derivation and proof of the 19 marker ruler. *IEEE Transactions on Information Theory.* 44:1. P. 379–382.

GAGLIARDI, R., ROBBINS, J. et TAYLOR, H. (1987). Acquisition sequences in PPM communications. *IEEE Transactions on Information Theory.* IT-33:5. P. 738–744.

GALINIER, P. et JAUMARD, B. (2006). A tabu search algorithm for difference triangle sets and golomb ruler problem. *Computers and Operations Research.* 33. P. 955–970.

GAREY, M. R. et JOHNSON, D. S. (1979). *« Computers and Intractability : A Guide to the Theory of NP-Completeness ».* W. H. Freeman and Company.

GIBBS, R. A. et SLATER, P. J. (1991). Distinct distance sets in a graph. *Discrete Mathematics.* 93:2-3. P. 155–165.

GOLOMB, S. W. (1972). How to number a graph. *Graph Theory and Computing.* New York : Academic Press. P. 23–37.

GRAF, A. (1998). Distance graphs and the T-coloring problem. *Discrete Mathematics.* 196:1-3. P. 153–166.

HACCOUN, D., CARDINAL, C. et GAGNON, F. (2005). Search and determination of convolutional self-doubly orthogonal codes for iterative threshold decoding. *IEEE Transactions on Communications.* 55:5. P. 802–809.

HAJÓS, G. (1961). Über eine konstruktion nicht n-färbbarer graphen. *Wiss. Z. Martin Luther Univ. Halle-Wittenberg Math.Natur.Reihe.*. 10. P. 116–117.

HALE, W. K. (1980). Frequency assignment : theory and applications. *Proc. IEEE.* 68:12. P. 1497–1514.

HANSEN, P., JAUMARD, B. et MEYER, C. (1999). On lower bounds for numbered complete graphs. *Discrete Applied Mathematics.* 94:1-3. P. 205–225.

HARARY, F. (1969). *« Graph Theory »*. Addison-Wesley Publishing Company.

HARARY, F., HEDETNIEMI, S. et PRINS, G. (1967). An interpolation theorem for graphical homomorphisms. *Portugal. Math.*. 26. P. 453–462.

HELL, P. et NEŠETŘIL, J. (1986). *On the complexity of H-coloring.* British Columbia : Simon Fraser University. TR-86-4.

HELL, P. et NEŠETŘIL, J. (2004). *« Graphs and Homomorphisms »*. Oxford University Press.

HOA, S. C. (1999). *Construction de règles de Golomb optimales.* Mémoire de maîtrise, École Polytechnique de Montréal.

HU, S. J., JUAN, S. et CHANG, G. J. (1999). T-colorings and T-edge spans of graphs. *Graphs and Combinatorics.* 15:3. P. 295–301.

HUANG, J. H. et SKIENA, S. S. (1994). Gracefully labelling prisms. *Ars Combinatoria.* 38. P. 225–242.

JANCZEWSKI, R. (2001). Divisibility and T-span of graphs. *Discrete Mathematics.* 234:1-3. P. 171–179.

JANSEN, K. (1996). A rainbow about T-colorings for complete graphs. *Discrete Mathematics.* 154:1-3. P. 129–139.

JENSEN, R. T. et TOFT, B. (1995). *« Graph Coloring Problems ».* John Wiley and sons.

KLIEBER, E. J. (1970). Some difference triangles for constructing self-orthogonal codes. *IEEE Transactions on Information Theory.* IT-16. P. 237–238.

KLONOWSKA, K., LUNDBERG, L. et LENNERSTAD, H. (2003). Using Golomb rulers for optimal recovery schemes in fault tolerant distributed computing. *IEEE Proceedings of the International Parallel and Distributed Processing Symposium.*

KLØVE, T. (1988). Bounds on size of optimal difference triangle sets. *IEEE Transactions on Information Theory.* 34:2. P. 355–361.

KLØVE, T. (1989). Bounds and construction for difference triangle sets. *IEEE Transactions on Information Theory.* 35:4. P. 879–886.

KLØVE, T. (1990). Bounds and constructions of disjoint sets of distinct difference sets. *IEEE Transactions on Information Theory.* 36:1. P. 184–190.

KOTZIG, A. et TURGEON, J. M. (1979). Perfect systems of difference sets and additive sequence of permutations. *Congressus Numerantium 24.* II. P. 629–636.

KOTZIG, A. et TURGEON, J. M. (1982). Construction of additive sequence of permutations of arbitrary lengths. *Annals of Discrete Mathematics*. 12. P. 239–242.

LAM, A. W. et SARWATE, D. V. (1988). On optimum time-hopping pattern. *IEEE Transactions on Communications*. COM-36:3. P. 380–382.

LAUFER, P. J. (1982). Regular perfect systems of difference sets of size 4 and extremal systems of size 3. *Annals of Discrete Mathematics*. 12. P. 193–201.

LIDL, R. et NIEDERREITER, H. (1994). *« Introduction to finite fields and their applications »*. Cambridge University Press.

LING, A. C. H. (2002). Difference triangle sets from affine planes. *IEEE Transactions on Information Theory*. 48:8. P. 2399–2401.

LIU, D. D. F. (1991). *Graph homomorphisms and the channel assignment problem.* Thèse de doctorat, University of South Carolina.

LIU, D. D. F. (1992). T-colorings of graphs. *Discrete Mathematics*. 101:1-3. P. 203–212. Special volume to mark the centennial of Julius Petersen's "Die Theorie der regulären Graphs", Part II.

LIU, D. D. F. (1996). T-graphs and the channel assignment problem. *Discrete Mathematics*. 161:1-3. P. 197–205.

LORENTZEN, R. et NILSEN, R. (1991). Application of linear programming to the optimal difference triangle set problem. *IEEE Transactions on Information Theory*. 37:5. P. 1486–1488.

MARTIN, G. D. (1985). Optimal convolutional self-orthogonal codes with an application to digital radio. *Proceedings of the IEEE International Conference on Communications.* P. 1249–1253.

MASSEY, J. L. (1963). *« Threshold Decoding »*. Cambridge, MA : MIT Press.

MATHON, R. (1987). Constructions for cyclic steiner 2-designs. *Annals of Discrete Mathematics.* 34. P. 353–362.

ROBERTS, F. (1991*a*). « From garbage to rainbows : Generalizations of graph colorings and their applications ». *Y. Alavi, G. Chartrand, O.R. Oellermann and A.J. Schwenk (eds.).* Wiley, New York. 2 de *Graph Theory, Combinatorics and Applications*, P. 1031–1052.

ROBERTS, F. (1991*b*). T-colorings of graphs : Recent results and open problems. *Discrete Mathematics.* 93. P. 229–245.

ROBINSON, J. P. et BERNSTEIN, A. J. (1967). A class of binary recurrent codes with limited error propagation. *IEEE Transactions on Computers.* 13:1. P. 106–113.

ROGERS, D. G. (1981). Addition theorems for perfect systems of difference sets. *Journal of London Mathematical Society.* 23. P. 385–395.

SHEARER, J. B. (1999). Improved LP lower bounds for difference triangle sets. *The Electronic Journal of Combinatorics.* RESEARCH PAPER 31.

SHEARER, J. B. n.d. *http ://www.research.ibm.com/people/s/shearer/home.html.*

SINGER, J. (1938). A theorem in finite projective geometry and some applications to number theory. *Trans. Amer. Math. Soc.*. 43. P. 377–385.

SKOLEM, T. (1957). On certain distribution of integers into pairs with given differences. *Mathematica Scandinavia.* 5. P. 57–68.

TESMAN, B. A. (1989). *T-colorings, list T-colorings, and set T-coloring of graphs.* Thèse de doctorat, Rutgers University.

TESMAN, B. A. (1990). Application of forbidden difference graphs to T-colorings. *Congressus Numerantium.* 74. P. 15–24.

TOWNSEND, R. L. et WELDON, E. J. (1967). Self-orthogonal quasi-cyclic codes. *IEEE Transactions on Information Theory.* IT-13. P. 183–195.

VANDERBECK, F. (2000). On dantzig-wolfe decomposition in integer programming and ways to perform branching in a branch-and-price algorithm. *Operations Research.* 48:1. P. 111–128.

WU, W. W. (1975). New convolutionnal codes-part 1. *IEEE Transactions on Information Theory.* 23:9. P. 942–955.

WU, W. W. (1976). New convolutionnal codes-part 2. *IEEE Transactions on Information Theory.* 24:1. P. 19–33.

ZHANG, J. G. (1999). Design of a special family of optical CDMA address codes for fully asynchronous data communications. *IEEE Transactions on Communications.* 47. P. 967–973.